IBM Systems - iSeries

セキュリティー
侵入検知

バージョン 5 リリース 4

IBM Systems - iSeries

セキュリティー
侵入検知

バージョン 5 リリース 4

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、 17 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、i5/OS (プロダクト番号 5722–SS1) のバージョン 5、リリース 4、モディフィケーション 0 に適用されます。また、改訂版で断りがない限り、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も適用されます。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。

本マニュアルに関するご意見やご感想は、次の URL からお送りください。今後の参考にさせていただきます。

http://www.ibm.com/jp/manuals/main/mail.html

なお、日本 IBM 発行のマニュアルはインターネット経由でもご購入いただけます。詳しくは

http://www.ibm.com/jp/manuals/ の「ご注文について」をご覧ください。

(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： IBM Systems - iSeries
Security Intrusion detection
Version 5 Release 4

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 2006.2

この文書では、平成明朝体™W3、平成明朝体™W7、平成明朝体™W9、平成角ゴシック体™W3、平成角ゴシック体™W5、および平成角ゴシック体™W7を使用しています。この(書体*)は、(財) 日本規格協会と使用契約を締結し使用しているものです。フォントとして無断複製することは禁止されています。

注* 平成明朝体™W3、平成明朝体™W7、平成明朝体™W9、平成角ゴシック体™W3、平成角ゴシック体™W5、平成角ゴシック体™W7

目次

侵入検知

侵入検知は、TCP/IP ネットワークを介して行われる無許可アクセス試行および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。セキュリティー管理者は、侵入検知によって提供される監査レコードを分析して、このタイプのアタックから iSeries™ ネットワークを保護することができます。

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) ということがあります。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ります。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、アクセス試行の検知、および、アタックの振る舞いの検知が侵入検知の重要な部分になります。

ユーザーは、TCP/IP ネットワークを介して入ってくる疑わしい侵入イベントを監査する侵入検知ポリシーを作成することができます。侵入検知機能が見つけ出す問題の例には、以下のものがあります。

- サービス妨害攻撃
- ポート・スキャン
- 誤った形式のパケット
- インターネット・プロトコル (IP) のフラグメント
- 制限された IP オプションおよびプロトコル
- Internet Control Message Protocol (ICMP) リダイレクト・メッセージ
- ユーザー・データグラム・プロトコル (UDP) ポート 7 (エコー・ポート) に対する永続エコー・アタック

また、監査データを分析し、TCP/IP 侵入が行われそうであるかどうかをセキュリティー管理者に報告するアプリケーションを作成することもできます。

重要: 侵入検知 という用語は、 iSeries 資料では、2 つの意味で使用されます。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権限を持ちすぎて、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、新規侵入検知機能を指します。

V5R4 の新機能

V5R4 では、侵入検知のトピック全体が新規です。

侵入検知

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を検知し、監査レコードを作成できます。

以下の侵入検知機能を実行して、システムを機密保護機能のある状態に保持できます。

- TCP/IP ネットワークに対する無許可アクセス試行およびアタックの特定タイプをモニターする侵入検知ポリシーを、 idspolicy.conf ファイルに作成します。
- 疑わしい侵入活動を監査します。
- 監査データを分析し、TCP/IP 侵入が行われそうであるかどうかについてセキュリティー管理者に勧告します。

新機能または変更点の確認方法

侵入検知に関するトピックは全体が新規であるので、本書ではリビジョン・バーは使用されていません。

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。

印刷可能な PDF

本書の PDF を表示およびプリントするには、以下の説明を使用してください。

本書の PDF バージョンを表示あるいはダウンロードするには、「侵入検知」を選択します。

次のような関連トピックを表示またはダウンロードできます。

- 「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、ほか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。
- 「QoS (Quality of Service)」。この資料には、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。

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. ブラウザーで PDF を右クリックする (上記の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

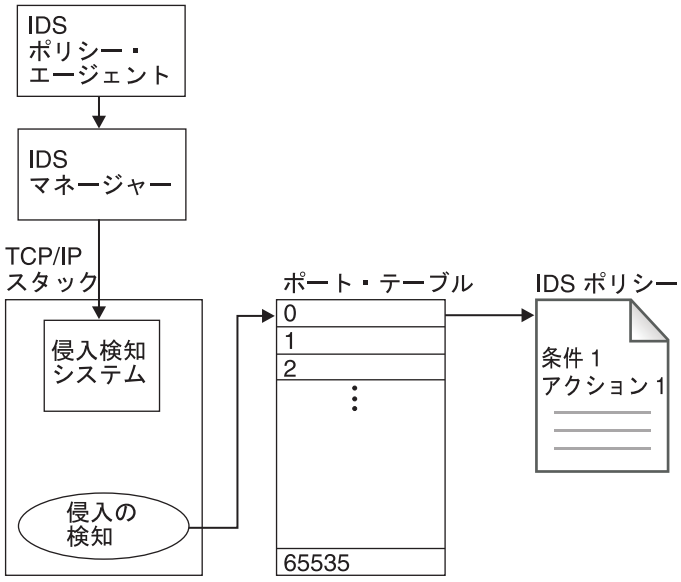
PDF を表示または印刷するには、システムに Adobe Reader がインストールされている必要があります。

Adobe Web サイト (www.adobe.com/products/acrobat/readstep.html) から、無償コピーをダウンロードできます。

概念

このトピックでは、侵入検知システムがどのようにはたらくかについて説明します。

侵入検知は、侵入イベント用に使用するポリシーのセットが入っている idspolicy.conf ファイルを使用します。各ポリシーは、関連した条件およびアクションを使用しますが、1 つのアクションに関連して複数の条件がある場合があります。 TCP/IP スタックは、最も一般的で潜在的な侵入イベントについて報告しその監査をするので、ユーザーは、データを分析し侵入が行われそうであるかどうかをセキュリティー管理者に報告するアプリケーションを作成できます。次の図は、侵入検知機能がどのようにはたらくかを示しています。



RZAUB500-0

1. idspolicy.conf ファイルを編集して特定タイプの侵入があるか検出し、次に QoS サーバーを始動します。
2. QoS ポリシー・エージェントが、idspolicy.conf ファイルの中の侵入検知ポリシーを読み取ります。
3. QoS ポリシー・エージェントが、マシン・インストラクション付きのメッセージを QoS マネージャーに送信します。
4. QoS マネージャーはマシン・インストラクションを解釈し、TCP/IP スタックの中にある侵入検知システムに送信します。 TCP/IP スタックはネットワーク内のアウトバウンド・トラフィックおよびインバウンド・トラフィックを管理し、ネットワーク内のその他のコンピューターに要求を経路指定します。
5. 侵入検知システムは、ポート・テーブル内にポリシーを作成します。ポート・テーブルの項目は、ポート 0 からポート 65 535 を表します。たとえば、すべてのポートに適用される条件が入っている ポート 0 は、侵入条件 1 を指し、侵入条件 1 はアクション 1 を指します。同様に、ポート 1 は条件 2 を指し、条件 2 はアクション 2 を指します。また、ポート 1 は条件 3 を指し、条件 3 はアクション 1 を指します。以下同様。
6. TCP/IP スタックは、侵入を検出すると、ポート・テーブルにマッチング条件があるか探し、特定のアクション、たとえば、IM 監査レコードまたはシステム統計などの作成を実行します。
7. システムは、侵入イベントのタイプを記述する IM 監査レコードを作成します。
8. システム管理者は IM 監査レコードを分析し、どのようなセキュリティー・アクション (たとえば、侵入の発生元のポートをクローズするなど) をとるべきかを決定します。

用語

このトピックでは、侵入検知の用語の定義について説明します。

サービス妨害 (DOS) アタック
コンピューター・セキュリティーにおいて、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。ネットワーク・サービスは、ある期間、中断されます。

Internet Control Message Protocol (ICMP)
たとえば、データグラムのエラーを報告するために、ゲートウェイによってソース・ホストとの通信に使用されるインターネット・プロトコル。

ICMP スキャン
システムを過負荷にする目的で ICMP を使用しようとするアタック。これは典型的なサービス妨害攻撃になります。

侵入検知
多岐にわたる望ましくない活動の検出を指す広義の用語。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る。あるアタックは、ターゲット・システムによって検知され、制圧される。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る。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ある。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く、アタックが行われたことが気付かれない。これらの理由で、情報収集、アクセス試行、およびアタックの振る舞いを検出することが、侵入検知の重要な要素になる。

ポート・スキャン
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。

Quality of Service (QoS)
トラフィック優先順位付けの指定ができる操作。QoS を使用することにより、ネットワーク全体にわたるさまざまなトラフィックを分類し管理できます。

トラフィック規定 (TR)
侵入検知ポリシー用に使用され、データ/接続の速度のしきい値を指定する。

ユーザー・データグラム・プロトコル (UDP)
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・サービスを提供する。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。

新規侵入検知ポリシーのセットアップ

ここでは、初めて侵入検知ポリシーをセットアップする方法について説明します。

侵入検知 (IDS) ポリシーは、以下の 2 つの部分で構成されます。

- IDS ポリシーに適用される条件 (たとえば、ポート、プロトコル、または IP アドレスなど) を示す IDS 条件。

- 条件が満たされたときにとるべきアクションを示す IDS アクション。複数の条件が 1 つのアクションを指すことができます。

IDS ポリシー・ファイル idspolicy.conf は、 i5/OS™ システムと一緒に配送され、/QIBM/ProdData/OS400/QOS/idspolicy.conf ディレクトリーに保管されています。サンプルの IDS ポリシー (コメント化されています) が、この配送済みファイルに組み込まれています。

/QIBM/UserData/OS400/QOS/ETC/ ディレクトリーおよび idspolicy.conf ファイルにアクセスできる権限を持っていることを確認してください。初めて侵入検知ポリシーをセットアップするには、以下のステップを実行します。

1. 以下のコマンドを実行して、IP QoS の使用可能性を「はい」に設定します。 `CHGTCPA IPQOSENB(*YES)`
2. WRKSYSVAL コマンドを実行して監査システム値を設定します。すると、システム値のリストが表示されます。
   a. `2` と入力し、QAUDLVL システム値の監査オプションを表示します。
   b. 監査オプションのリストに `*ATNEVT` を追加します。

      QAUDLVL に *ATNEVT を設定する余裕がない場合は、下に説明されているように、QAUDLVL に *AUDLVL2 が設定されていることを確認してください。PF3 を押して終了します。
   c. `2` と入力し、QAUDLVL2 システム値の監査オプションを表示します。
   d. 監査オプションのリストに `*ATNEVT` を追加します。PF3 を押して終了します。
3. IDS ポリシー・ファイルを構成するために、ファイルを /QIBM/ProdData/OS400/QOS/idspolicy.conf から /QIBM/UserData/OS400/QOS/ETC/ にコピーします。
4. IDS ポリシー・ファイルを編集します。
5. 次のコマンドを使用して QoS サーバーを始動します。 `strtcpsvr *qos`

   QoS サーバーは、始動されると、ETC ディレクトリーの中を見て、idspolicy.conf ファイルがあるか調べます。 idspolicy.conf ファイルがない場合は、idspolicy.conf ファイルは、/QIBM/ProdData/OS400/QOS/ ディレクトリーから /QIBM/UserData/OS400/QOS/ETC/ ディレクトリーにコピーされます。
6. 活動ジョブの処理 (Work with Active Jobs) (WRKACTJOB) コマンドを実行して、QoS サーバーが開始されていることを確認します。開始済みサーバーのリストに QTOQSRVR が表示されます。

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。

関連資料

7 ページの『IDS ポリシー・ファイル内のキーワード』
IDS ポリシー・ファイル内のキーワードのほとんどはこのリリースでサポートされていますが、 サポートされていないキーワードがいくつかあります。

侵入検知ポリシー・ファイルの変更

ここでは、侵入検知ポリシー・ファイルを変更するために実行するステップについて説明します。

以下のステップを実行して侵入検知ポリシー・ファイルを編集します。

1. 次のコマンドを使用して QoS サーバーを停止します。 `endtcpsvr *qos`
2. /QIBM/UserData/OS400/QOS/ETC/ ディレクトリーにある IDS ポリシー・ファイルを編集します。
3. 次のコマンドを使用して QoS サーバーを始動します。 `strtcpsvr *qos`

4. 活動ジョブの処理 (Work with Active Jobs) (WRKACTJOB) コマンドを実行して、QoS サーバーが開始されていることを確認します。開始済みサーバーのリストに QTOQSRVR が表示されます。

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サンプルは、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ークと相関関係をとります。侵入検知システムは統計を生成し、ユーザー指定しきい値が超えられると、システムは監査レコードを生成します。 IDS ポリシー・ファイルの中の ibm-idsMaxEventMessage パラメーターを使用して、監査ジャーナルに書き込まれるレコードの数を制限してください。

このポリシーでは、単一の IDS トラフィック規定 (TR) 条件と単一の IDS アクションを指しています。この IDS 条件では、TCP プロトコル、ローカル・ポート 8000、およびローカル・ホスト IP アドレスが選択されます。

IDS アクションでは、リスニング・サーバー用に 1000 という TCP 接続制限、10 分の統計間隔、および TR 接続の 10 パーセントが指定されています。この例では、ローカル・ホスト IP アドレスが、9.10.11.000 から 9.10.11.255 の範囲のアドレスとして示されています。

```
 ibm-idsConditionAuxClass     rule1     # IDS condition
 {
 ibm-idsConditionType         TR
 ibm-idsLocalPortRange        8000
 ibm-idsProtocolRange         6
 ibm-idsLocalHostIPAddress    2-9.10.11.000-24
 policyIdsActionName          idsact1
 }

 ibm_idsActionAuxClass        idsact1   # IDS action
 {
 ibm-idsActionType            TR
 ibm-idsStatInterval          10
 ibm-idsTRtcpTotalConnections 1000
 ibm-idsTRtcpPercentage       10
}
```

例: 制限された IP プロトコル・ポリシー

この例は、200 から 205 の範囲の制限された IP プロトコル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。

```
 ibm-idsConditionAuxClass     idscond4   # IDS condition
{
ibm-idsConditionType         ATTACK
ibm-idsAttackType            RESTRICTED_IP_OPTIONS
ibm-idsProtocolRange         200-205
ibm-policyIdsActionName      idsact2
}

 ibm-idsActionAuxClass        idsact2
 {
 ibm-idsActionType            ATTACK
 ibm-idsMaxEventMessage       5
 }
```

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。

この例では、 6 ページの『例: 制限された IP プロトコル・ポリシー』の例と同じ IDS アクション idsact2 を使用します。

```
ibm-idsConditionAuxClass    idscond5   # IDS condition
{
ibm-idsConditionType        ATTACK
ibm-idsAttackType           PERPETUAL_ECHO
ibm-idsLocalPortRange       7
ibm-idsRemotePortRange      7
ibm-policyIdsActionName     idsact2
}
```

例: 侵入検知スキャン・ポリシー

この例は、独立の条件とアクションを使用するスキャン・ポリシーの例です。

TCP/IP スタックは、ポートごとのベースでポート・スキャンを検出します。スタック自体でグローバル・スキャンを検出することはできません。ポート・スキャンが疑われると、スタックは SCAN_EVENT を生成し、これが侵入検知システムを呼び出します。侵入検知システムはスキャン・イベントを処理し、SCAN_GLOBAL コードを呼び出して統計を生成し、しきい値をモニターします。

次に示す IDS ポリシーは TCP 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。

```
ibm-idsConditionAuxClass     idscond10  # IDS condition
{
ibm-idsConditionType         SCAN_EVENT
ibm-policyIdsActionName      idsscan1
ibm-idsProtocolRange         6
ibm-idsLocalPortRange        1-5000
}
ibm-idsActionAuxClass        idsscan1   # IDS action
{
ibm-idsActionType            SCAN_GLOBAL
ibm-idsFSInterval            10
ibm-idsFSThreshold           10         # fast scanning threshold
ibm-idsSSInterval            100
ibm-idsSSThreshold           20         # slow scanning threshold
}
```

IDS ポリシー・ファイル内のキーワード

IDS ポリシー・ファイル内のキーワードのほとんどはこのリリースでサポートされていますが、サポートされていないキーワードがいくつかあります。

サポートされているキーワード

IDS ポリシーには、サポートされている以下のキーワードが入っています。

- ibm-policyIdsActionName
- ibm-idsICMPRedirect
- ibm-idsConditionAuxClass
- ibm-idsConditionType
- ibm-idsAttackType
- ibm-idsLocalPortRange

- ibm-idsRemotePortRange
- ibm-idsProtocolRange
- ibm-idsIPOptionRange
- ibm-idsLocalHostIPAddress
- ibm-idsRemoteHostIPAddress
- ibm-idsActionAuxClass
- ibm-idsActionType
- ibm-idsStatInterval
- ibm-idsMaxEventMessage
- ibm-idsTRtcpTotalConnections
- ibm-idsTRtcpPercentage
- ibm-idsTRtcpLimitScope
- ibm-idsTRudpQueueSize
- ibm-idsFSInterval
- ibm-idsFSThreshold
- ibm-idsSSInterval
- ibm-idsSSThreshold

IDS ポリシー・ファイルにある以下のキーワードは、許可されていますが、このリリースでは無視されます。

ibm-idsMessageDest
IDS によって生成されたメッセージをどの待ち行列に入れるかを示します。 (すべてのメッセージは監査レコードに入れられ、待ち行列には送信されません。)

ibm-idsNotification
ログ・ファイルまたはコンソールが通知されるかどうかを示します。 (すべてのメッセージが監査ジャーナルにのみ入れられます。)

ibm-idsLoggingLevel
ログ・ファイルにログ記録されるメッセージの数の制限を示します。

ibm-idsTypeActions
ある条件に対してとるべきアクションのタイプを示します。 (とられる唯一のアクションは、監査レコードを作成することです。)

ibm-idsSensitivity
条件の優先順位を示します。 (すべての条件は、等しい優先順位を持っているものとして扱われます。)

ibm-idsScanExclusion
スキャンが検出された場合に統計収集の記帳から除外される IP アドレスとポートの配列を示します。スキャン・イベントに関連付けられている IP アドレスまたはポートは、統計から除外されることはありません。

関連タスク

4 ページの『新規侵入検知ポリシーのセットアップ』
ここでは、初めて侵入検知ポリシーをセットアップする方法について説明します。

侵入検知ポリシー・ファイルのバックアップ

侵入検知 (IDS) ポリシーは、サーバー停止または電源障害が起こった場合にポリシーを再作成せずにすむように、バックアップをとっておきます。

IDS 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。 IDS ポリシーは、以下のディレクトリーにバックアップをとっておくことをお勧めします。

QIBM/UserData/OS400/QOS/ETC

QIBM/ProdData/OS400/QOS/

また、QoS サーバーのディレクトリー・サーバー出版エージェントのバックアップをとる必要があります。出版エージェントには、ディレクトリー・サーバー名、QoS サーバーの識別名 (DN)、ディレクトリー・サーバーにアクセスするのに使用するポート、および認証情報が入ります。ポリシー・ファイルを逸失した場合、バックアップをとっておくと、ポリシーを最初から再作成するのにかかる時間と作業を節約できます。

以下のステップを実行して、失った IDS ポリシーを簡単に置き換えられるようにしてください。

1. **統合ファイル・システムのバックアップおよび回復プログラムの使用。**

   「*バックアップおよび回復*」には、統合ファイル・システムからバックアップを実行するための説明があります。

2. **ポリシーの印刷。**

   印刷出力を機密保護機能のある場所に保管し、必要に応じて情報を再入力できます。

3. **ディスクへの情報のコピー。**

   コピーのほうが印刷出力よりも利点があります。手動で再入力するかわりに、電子的に存在している情報を使用できるからです。また、これにより、あるオンライン・ソースから別のソースに情報をトランスポートする簡単な方法が提供されます。

   関連情報

   バックアップおよび回復 PDF

侵入検知ポリシー・ファイルの管理

システム管理者に E メールを送信するように侵入検知プログラムを構成し、疑わしいイベントについてシステム管理者にアラートし、とるべきアクションについての提案を提供できます。

また、あるパターンの場合の統計を分析するプログラムを作成することもできます。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必要があります。たとえば、ルーターの構成がまだ完了していないことを ICMP リダイレクト・メッセージが示すことができます。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。

侵入検知活動の監査

侵入検知活動の監査方法について説明します。侵入検知システム (IDS) が疑わしいイベントを検出してフラグを立てた場合、IDS は IM 監査レコードを書き込みます。

QAUDCTL システム値に *AUDLVL があり、さらに QAUDLVL または QAUDLVL2 システム値に *ATNEVT がある場合は、必ず監査レコードがセキュリティー監査ジャーナルに書き込まれます。

注: QAUDLVL2 に *ATNEVT を設定するには、まず、QAUDLVL に *AUDLVL2 を設定する必要があります。

IM 監査レコードを表示するには、以下のステップを実行します。

1. 次のコマンドをコマンド行から実行して、監査ジャーナルのすべてを表示します。 `DSPJRN QAUDJRN`

   タイプ M の監査レコードがある場合は、IDS が疑わしいイベントを検出してフラグを立てたことを意味します。 IM 監査レコードが表示されない場合、IDS が疑わしいイベントを検出しなかったことを示します。 (IM 監査レコードのみを表示するには、`DSPJRN QAUDJRN ENTTYP(IM)` コマンドを実行します。)
2. 5 と入力し、IM 監査レコードの内容を表示します。
3. 疑わしいイベントをシステム管理者に報告し、適切なアクション (たとえば、ポートをクローズする、またはスプーフされた IP アドレスをトラッキングする) をとるように依頼します。

これで、IM 監査レコードを分析する準備ができました。監査レコードを使用することが、疑わしいイベントが起こったことをシステム管理者にアラートできる唯一の方法です。

注: IM レコード内のいくつかのフィールドは 16 進形式になっています。これらの 16 進フィールドを表示するには、F11 を押します。

関連資料

11 ページの『監査データの分析』
侵入検知活動の監査データの分析方法、 および、IM 監査レコード内のフィールドについての参照情報の入手方法について説明します。

監査データの分析

侵入検知活動の監査データの分析方法、および、IM 監査レコード内のフィールドについての参照情報の入手方法について説明します。

次の例には、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 . . . . . . . . . .:   5
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    'QSNADS1003QUSRSYS   '
00001    'P2005-06-06-15.01.32.6482729999 000009.10.11.0    '
00051    '                                000009.10.11.255'
00101    '                         ,        ATTACK    RESTP'
00151    'ROT
```

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。

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	サンプル項目
項目タイプ	Char(1)	潜在的な侵入イベントが検出されました。	P
イベントの時刻	TIMESTAMP	イベントが検出された時点のタイム・スタンプ。	2005-06-06-15.01.32.648272
検出点の識別コード	Char(4)	侵入イベントを検出したプロセッシング・ロケーションの固有 ID。このフィールドはサービス担当員が使用します。	9999
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。	このフィールドは非表示で、ブランクのように見えます。情報を表示するには、F11 を押します。
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。 (ゼロ (0) というポートはないので、00000 という値は、いずれかのポートに侵入があったことを表します。)	00000
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。	9.10.11.0
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。	このフィールドは非表示で、ブランクのように見えます。情報を表示するには、F11 を押します。
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。	00000
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。	9.10.11.255

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	サンプル項目
プローブ・タイプ識別コード	Char(6)	潜在的な侵入を検出するために使用されるプローブのタイプを示します。可能な値には、次のものがあります。 **ATTACK** アタック・アクション・イベント **TR** トラフィック規定トレース・アクション・イベント **SCANG** スキャン・グローバル・アクション・イベント **SCANE** スキャン・イベント・アクション・イベント	ATTACK
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。この識別コードを使用して、この監査レコードをその他の侵入検知情報と相互に関連させることができます。	このフィールドは非表示で、ブランクのように見えます。情報を表示するには、F11 を押します。
イベント・タイプ	Char(8)	検出された潜在的な侵入のタイプを示します。可能な値には、次のものがあります。 **MALFPKT** 誤った形式のパケット **FLOOD** フラッディング・イベント **ICMPRED** Internet Control Message Protocol (ICMP) リダイレクト **PERPECH** 永続エコー **IPFRAG** IP フラグメント **RESTPROT** 制限された IP プロトコル (RESTP)	RESTP
疑わしいパケット	Char(1002)	この可変長の 2 進数フィールドには、検出されたイベントに関連した IP パケットの最初の 1000 バイト (最大) が入ります。このフィールドの最初の 2 バイトには疑わしいパケット情報の長さが入ります。	このフィールドは非表示で、ブランクのように見えます。情報を表示するには、F11 を押します。

関連タスク

10 ページの『侵入検知活動の監査』
侵入検知活動の監査方法について説明します。 侵入検知システム (IDS) が疑わしいイベントを検出してフラグを立てた場合、IDS は IM 監査レコードを書き込みます。

スキャン・イベント

侵入検知システムは、個々のポートに対するスキャンを検出します。

侵入検知システムは、統計の収集および監査を使用して、システムがグローバル・スキャンのターゲットであったかどうかを判別します。侵入イベントが検出されたことを TCP/IP スタックが検知すると、スタックは侵入検知機能を呼び出し、統計と監査レコードを生成します。

IDS ポリシー・ファイルに IDS スキャン・ポリシーがない場合、アクションはとられません。 IDS スキャン・ポリシーがある場合、侵入検知システムは、スキャン・イベントを検出すると、監査レコードを作成します。

TCP ポート・スキャン

TCP イベントは、「通常」、「疑わしい可能性がある」、または「非常に疑わしい」と分類できます。IDS ポリシーに、だれも使用できない制限されたポートを定義することができます。

侵入検知システム (IDS) は、以下のタイプの TCP イベントをスキャンし、分類します。通常、TCP/IP スタックは疑わしいイベントを廃棄します。

表 2. 疑わしいと分類される TCP スキャン・イベント

スキャン・イベント	TCP/IP 接続状態	イベントの分類
どのパケットも受け取る	アンバインド済み、制限なし	疑わしい可能性がある (障害のあるアプリケーションである可能性がある)
TCP ヘッダーにリセット (RST) ビットが設定されたパケットを受け取る。(この状態では、ホストは即時に接続を終了し、その結果、接続が再確立されるまでサービス妨害になる。)	ハーフオープン接続	疑わしい可能性がある (ピアがトラックをカバーする)
最終タイムアウト	任意の接続状態	疑わしい可能性がある (ピアが接続を中止している)
予期しないフラグを受け取る	任意の接続状態	非常に疑わしい
制限された TCP/IP ポートから任意のパケットを受け取る	この TCP/IP ポートは RESERVED	非常に疑わしい
最終タイムアウト	ハーフオープン接続	非常に疑わしい (ピアがハンドシェークを中止している)

ユーザー・データグラム・プロトコル (UDP) ポート・スキャン

UDP イベントは、「通常」、「疑わしい可能性がある」、または「非常に疑わしい」と分類できます。IDS ポリシーに、だれも使用できない制限されたポートを定義することができます。制限されたポートで受け取られたデータグラムはすべて非常に疑わしいイベントとして扱われます。アンバインド済みで制限のないポートで受け取られたデータグラムは疑わしい可能性があるイベントとして扱われます。バインド済みポートで受け取られ、QoS ポリシーまたは FW フィルターでリジェクトされたデータグラムは、疑わしい可能性があるとして扱われます。バインド済みポートで受けられたその他のデータグラムはすべて通常イベントとして扱われます。

IDS ポリシー・ファイルに IDS スキャン・ポリシーがない場合、アクションはとられません。 IDS スキャン・ポリシーがある場合、侵入検知システムは、スキャン・イベントを検出すると、監査レコードを作成します。

表 3. UDP スキャン・イベント

スキャン・イベント	TCP/IP 接続状態	イベントの分類
QoS ポリシーがパケットをリジェクトする	バインド済み	通常
どのパケットも受け取る	バインド済み	通常
FW フィルター操作がパケットをリジェクトする	バインド済み	疑わしい可能性がある
どのパケットも受け取る	アンバインド済み	疑わしい可能性がある (障害のあるアプリケーションである可能性がある)
どのパケットも受け取る	この TCP/IP ポートは制限されている	非常に疑わしい

Internet Control Message Protocol (ICMP) ポート・スキャン

ICMP 要求を使用してネットワーク・トポロジーをマップすることができます。サブネット・ベースまたはブロードキャスト・アドレスに送信された要求はすべて非常に疑わしいイベントとして扱われます。エコー (ping) 要求およびタイム・スタンプ要求は、よくある要求であるので、通常イベントとして扱われます。侵入検知システムは ICMP リダイレクト・イベントを監査します。

アタック・イベント

侵入検知システムはさまざまなタイプのアタック・イベントを検出し、IM 監査レコードを QAUDJRN 監査ジャーナルに書き込みます。

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。
- 誤った形式のパケット
- サービス妨害フラッディング
- ICMP リダイレクト・メッセージ
- UDP ポートでの永続エコー
- IP フラグメント
- 制限された IP オプションおよびプロトコル
- フラグメント化されたパケット

システムが生成する監査レコードの数は、IDS ポリシー内の最大イベント・メッセージの値によって決まります。

誤った形式のパケット・イベント

誤った形式のパケットは、そのパケットが処理されるとシステムを破損するまたはハングするように作成されます。 IDS ポリシーは、誤った形式のパケットを検出すると、監査レコードを書き込みます。 TCP/IP スタックは、誤った形式のパケットを削除します。

フラグメント制限イベント

無効なフラグメントは、ファイアウォール検査をバイパスしようとするときに、IP ヘッダーまたはトランスポート・ヘッダーをオーバーレイします。 iSeries システムでは、IP ヘッダーをオーバーレイすることはできません。 TCP/IP スタックは、フラグメント化されたデータグラムの最初のフラグメントに最低 576 バイトあることを検査し確認します。また、スタックは、最初のフラグメントを超えた先のそれぞれのフラグメントが 256 バイトより大きいオフセットを使用していることを確認します。

IDS ポリシーは、無効の IP フラグメントを監査します。

IP オプションの制限

データグラム内の IP オプション・フィールドは可変長で、オプションの情報のリストを入れます。 IP オプションの一部、たとえば Loose Source Route は、ネットワークのアタックに使用することが可能です。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。たとえば、制限された IP オプションがあるインバウンド・パケットを無視するか監査するかを指定できます。また、制限された IP オプションがあるインバウンド・パケットの数についての統計を生成できます。

IP プロトコルの制限

IP プロトコル・フィールドは、IP ヘッダー内の 8 ビットのフィールドです。未定義の IP プロトコルが、ネットワークに対するバック・ドア・アタックを設定するために使用されることがしばしばあります。ユーザーは IDS ポリシーを使用して、インバウンド・パケットに入れることができる IP プロトコルを制限することができます。制限された IP プロトコルがあるインバウンド・パケットを監査するかどうかを、ポリシーで指定できます。また、制限された IP プロトコルがあるインバウンド・パケットの数についての統計を生成できます。

SYN フラッディング・イベント

TCP SYN フラッディング・イベントは、大量のハーフオープン・ソケットを作成します。これらのフラッディング・イベントは、所定のアプリケーションのソケット接続バックログを埋め、有効な接続が受け入れられるのを拒否します。 SYN フラッディング・イベントは、アクセス不可能なシステムのアドレスでソースの IP アドレスをスプーフします。 IDS ポリシーは、SYN フラッディング・イベントを検出するとフラグを立て、監査レコードを書き込みます。

ICMP リダイレクト・イベント

Internet Control Message Protocol (ICMP) リダイレクト・メッセージを使用して、意図されたネットワーク経路をオーバーライドできます。 IDS ポリシー・ファイルで、ICMP リダイレクト・メッセージを無視するか処理するかを IGNOREREDIRECT オプションで指定できます。

UDP ポートでの永続エコー

エコー・ポート と呼ばれるポート 7 を使用して、UDP 接続をテストできます。 (ソース・ポートおよびターゲット・ポートの両方をポート 7 に設定すると、これらのポート間でエコーが起こります。) UDP を使用して送信したデータはすべてエコー・バックされます。永続エコーは UDP ポート 7 に対するアタックになります。 TCP/IP スタックは、ソース・ポートがターゲット・ポートに等しい場合にこのイベントを検出します。アタック・タイプ・イベントに関する IDS ポリシーがある場合、システムは、UDP ポートに対する永続エコー・アタックを検出すると必ず監査レコードを書き込みます。

侵入検知の関連情報

このトピックには、侵入検知に関連したプロダクト・マニュアルおよび IBM® Redbooks™ (PDF 形式)、Web サイト、および Information Center トピックが記載されています。 PDF 資料は、いずれも、表示または印刷できます。

マニュアル

- 機密保護解説書

その他の情報

- 「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、ほか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。
- 「QoS (Quality of Service)」。この資料には、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。

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. ブラウザーで PDF を右クリックする (上記の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

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) から、無償コピーをダウンロードできます。

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。

〒106-0032
東京都港区六本木 3-2-31
IBM World Trade Asia Corporation
Licensing

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で提供し、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、お客様に対してなん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。

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が、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。

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 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、IBM Corporation の商標です。

e(ロゴ)server
eServer
i5/OS
IBM
IBM (ロゴ)
iSeries
Redbooks

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

お客様がご使用になる資料につきましては、以下の条件にしたがって、その使用が認められます。

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。本書は、特定物として現存するままの状態で提供され、第三者の権利の不侵害の保証、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

日本アイ・ビー・エム株式会社
〒106-8711　東京都港区六本木3-2-12