IBM i 2024

IBM i コンテンツ (2024年9月版)

鉄壁のIBM i へ、侵入を図る動きを検知!
IBM i のセキュリティー拡張機能（侵入検知機能）のご紹介

日本アイ・ビー・エム株式会社
テクノロジー事業本部
IBM Powerテクニカルセールス

鉄壁のIBM i へ、侵入を図る動きを検知!
IBM i のセキュリティー拡張機能（侵入検知機能）のご紹介

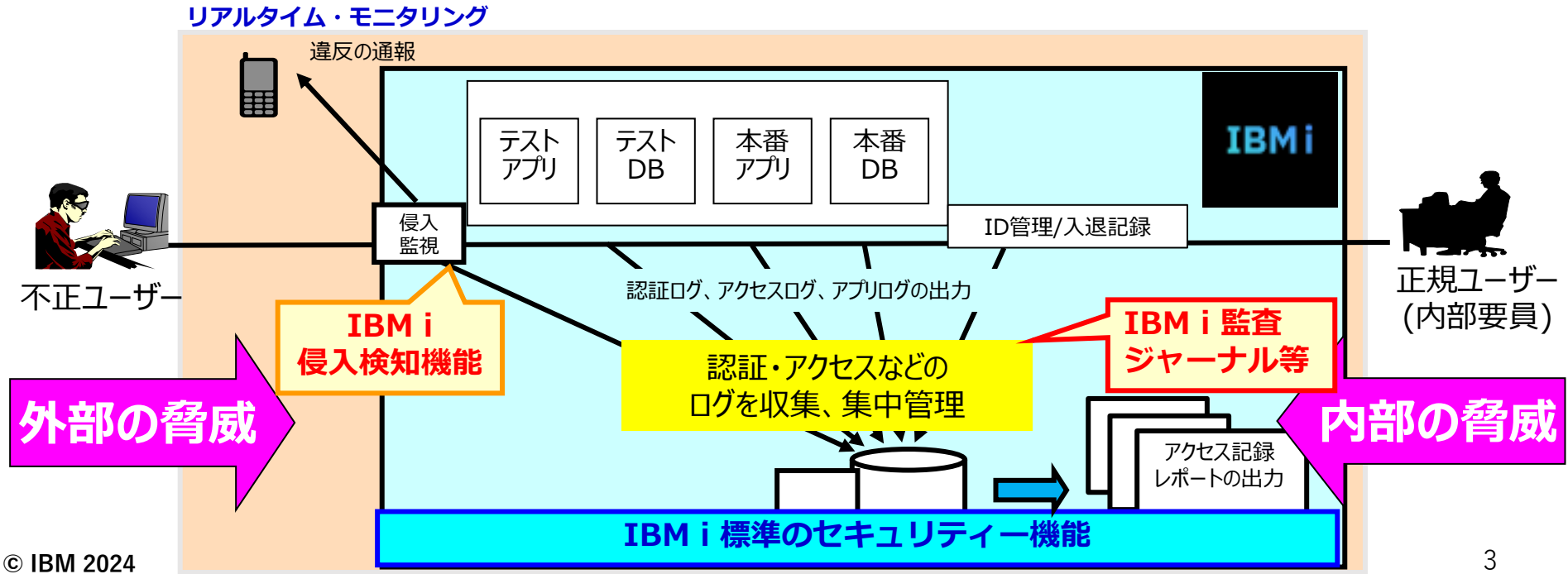
IBM i には、次のような外部、内部からの無数の脅威から保護するための、様々な組み込み機能があります。
主な機能をあげると下記になります。
・オブジェクト指向による、ウイルス耐性アーキテクチャー
・オブジェクトレベルの権限制御機能
・侵入検知機能(IDS)
・セキュリティ監査ジャーナル
・システム履歴ログ

7月のコラムでは、「セキュリティ監査ジャーナル」を
8月のコラムでは、「オブジェクトレベルの権限制御」を含む「基本的なセキュリティ機能」をご紹介しました。
9月のコラムでは、外部の脅威からの保護機能として、「侵入検知機能」をご紹介します。

目次

1. 抜け漏れのないセキュリティー・アーキテクチャー

- ✓ IBM i では 外部及び、内部からの脅威に対応して、下記の機能が実装されています。
  - ➢ 内部からの脅威：ユーザーID管理/入退記録管理/オブジェクトのアクセス管理と監査機能
  - ➢ 外部からの脅威：侵入検知機能



解説：

・内部からの脅威に対応した機能として、ユーザーID管理、入退記録、オブジェクト毎のアクセス権限と「監査ジャーナル等の管理」については、2024年7月と8月のPOWERコラムで、ご紹介しました。
https://www.jbcc.co.jp/products/solution/poweri/column/

・当資料では、主に、外部からの脅威への対応として、「侵入検知の機能」　についてご紹介します。

・侵入検知機能(IDS :Intrusion Detection Systemの略) 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が試行されたとき、それを通知します。
また、IDS は、ご使用の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出もモニターします。

・IBM iの侵入検知機能（IDS)は、ハッキング、マルウェア、DDoS攻撃などの外部からの攻撃から保護する強力なツールです。管理者は、トラフィックのしきい値を設定し、トラフィックが事前定義された量を超えたときに IDSから自動的に通知が送信されるようにすることができます。

2. IBM i の侵入検知機能とは

（1）概要

- ✓ IBM i では、侵入検知機能はOS標準機能　（IBM i 6.1以降）
- ✓ TCP/IP ネットワークを介して侵入す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できる
  - ➢ 侵入モニター(IM)レコードが、監査ジャーナルとしてログされる
- ✓ 侵入の防止ではなく、疑わしい侵入活動を監査する機能
- ✓ リアルタイム通知が可能
  - ➢ IMレコードに加えてe-mail,MSGQに送信

- ✓ GUIインターフェースのサポート
  - ➢ IBM Navigator for iによる設定で、監査ジャーナルを意識せずにイベント表示

解説：

・潜在的な侵入および侵出は、 セキュリティー監査ジャーナルに侵入モニター監査レコード（IM）として記録され、 侵入検知システムの IBM Navigator for iでは 侵入イベントとして表示されます。
IDS を構成して、侵入および侵出の発生を防止できます。
IDSの機能を使用するためには、監査ジャーナルを起動している必要があります。

・IBM Navigator for iの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。 （昔のIBM iのような）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。

・IBM Navigator for i を使用して、監査ジャーナルにログとして記録された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。

・IBM iの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。

→最新のPowerSC v2.2を利用すれば、アンチウィルス（ClamAV）によるウィルス検知が可能になっています。

https://www.ibm.com/docs/ja/powersc-standard/2.2?topic=security-configuring-anti-malware

2. IBM i 侵入検知機能

（2）検知できる侵入・侵出イベント

✓ IBM iで検知できるイベント一覧

- **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をモニターする。使用しているシステムがアタックされたり、アタックのソースとして利用されたりすることがある。
- **抽出イベント**
  抽出 は、ローカル・ホスト・システムからリモート・システムに対して発信される攻撃、トラフィック規定、またはスキャン・イベントです
- **スキャン・イベント**
  スキャンは、システムに侵入する方法を探すために、未使用のポートへの接続を試みる攻撃
- **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、確立された TCP 接続、ユーザー・データグラム・プロトコル (UDP) エラー、およびシステム SSL/TLS ハンドシェーク失敗をモニターする
- **可変動的スロットル**
  各侵入検知 (IDS) ポリシーで 可変動的スロットル を指定できます。 有効にされた 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る。

解説：

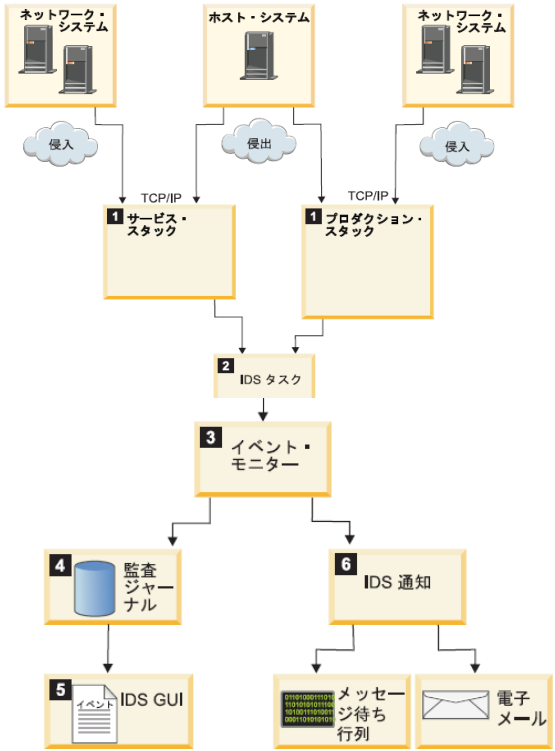
- **アタック・イベント**
  アタック・ポリシーは、システムに対するさまざまなタイプのアタックをモニターします。
  使用しているシステムがアタックされたり、アタックのソースとして利用されたりするおそれがあります。
  IDS はアタックを検知すると、侵入イベントを監査レコードに書き込みます。
- **抽出イベント**
  抽出 は、ローカル・ホスト・システムからリモート・システムに対して発信される攻撃、トラフィック規定、
  またはスキャン・イベントです。 例えば、信頼された内部関係者が、サービス妨害攻撃の発信元として会社のマシンを
  使用する可能性があります。 侵出は、アウトバウンド侵入 とも呼ばれます。
- **スキャン・イベント**
  スキャン は、システムに侵入する方法を探すために、未使用のポートへの接続を試みる攻撃です。 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。 開いているポートが見つかると、ハッカーは、システムの脆弱点を
  見つけて、アクセスを試みます。
- **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、確立された TCP 接続、ユーザー・データグラム・プロトコル (UDP) エラー、およびシステム
  SSL/TLS ハンドシェーク失敗をモニターします。 すべてまたは特定の IP アドレスおよびポートでポリシーを構成できます。
- **可変動的スロットル**
  各侵入検知 (IDS) ポリシーで 可変動的スロットル を指定できます。 有効にされた 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。

上記の詳細は、下記を参照してください。
https://www.ibm.com/docs/ja/i/7.5?topic=concepts-intrusion-extrusion-types

2. IBM i 侵入検知機能

（３）侵入検知機能が疑わしい侵入および侵出を検知報告するフロー

✓ IBM iで侵入を検知した場合



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出を検知すると、IDS タスクにイベントを送信

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、侵入および侵出イベントに関する統計を保持

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出のイベントを通知

4. イベントが通知されると、侵入モニター・レコードが監査ジャーナルに作成

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
6. 「IDS プロパティー(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。

解説：

・2-3のIDSタスクの補足です。侵入検知のみではなく、下記のような防御の機能もあります。

・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。有効にされた 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。

可変で動的なスロットルを有効にしている場合、IDSタスクは、侵入または侵出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知します。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。
- 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。

3. 侵入検知機能を使ってみよう

（1）「侵入検知ポリシー」の作成

✓ IBM Navigator for iの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してみよう。

①IBM Navigator for iの「セキュリティ」
→「侵入検知」→「ポリシーの管理」を選択

②侵入検知ポリシーを作成します。「アクション」→「NEW」を選択します。

解説：

・当資料でご紹介している、新しいGUIである、侵入検知システム用の IBM Navigator for i の操作を実施するためには、下記の最新PTFの適用が必要です。

HTTPサーバー用の Group PTFが下記のレベル以上である必要があります。

IBM i 7.3： HTTP SF99722 level 41
IBM i 7.4： HTTP SF99662 level 22
IBM i 7.5： HTTP SF99952 level 4

詳細は下記参照
https://www.ibm.com/support/pages/intrusion-detection-system-ids-ibm-i-new-navigator

・IBM® Navigator for iの侵入検知システム GUI を使用するには、以下の手順を実行します。
「セキュリティー」 >「 侵入検知」を展開します。
以下のタスクを実行できます。

-IDS の開始または停止
「侵入検知システム (Intrusion Detection System)」セットアップの管理
-侵入検知ポリシーの管理
-侵入検知イベントの表示

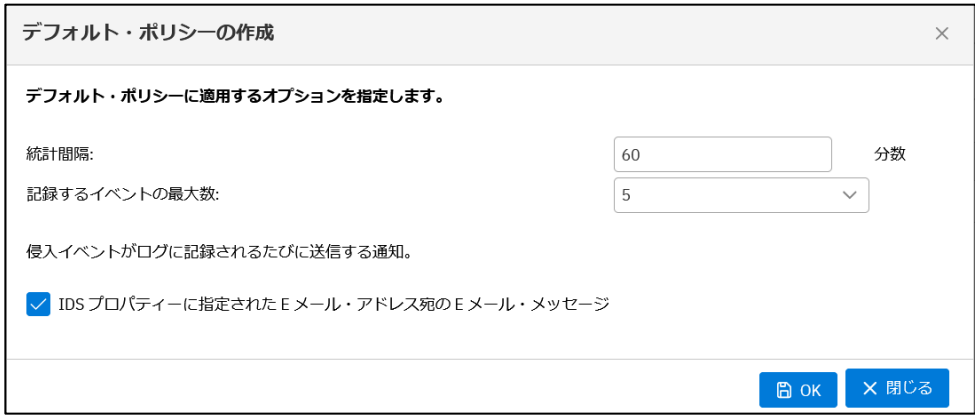
・侵入検知ポリシーを処理するには、*ALLOBJ および *IOSYSCFG 権限が必要です。

3. 侵入検知機能を使ってみよう

✓ 「デフォルトの侵入検知ポリシー・セット」を作成します。

③下記が表示されるので、「デフォルトの侵入検知ポリシーのセットを作成」を選択する。（下記のように選択し、[OK]）

④オプション（統計間隔とイベントの最大数）を指定します。下記のようにデフォルト値を選択して[OK]



解説：

・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知します。

・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制ポリシーを作成することもできます。それぞれを簡単に説明したのが下記になります。

-アタック・ポリシー：システムリソースを変更したり、その操作に影響を与えたりする意図的な試行の検出
-スキャン・ポリシー：システムに侵入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の検出
-トラフィック規制ポリシー：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の検出

3. 侵入検知機能を使ってみよう

✓ 「デフォルトの侵入検知ポリシー・セット」を作成します。

⑤下記のように表示されればOKです。

ポリシー名	デフォルト・ポリシー	ポリシー・タイプ	ステータス	ローカル IP アドレス	ローカル・ポート	リモート IP アドレス	リモート・ポ
フィルター		フィルター	フィルター	フィルター	フィルター	フィルター	フィルター
QIBM_Address_Poisoning	✓	アタック (Address Poisoning)	Enabled	All	All	All	All
QIBM_Flood	✓	アタック (Flood)	Enabled	All	All	All	All
QIBM_Fraggle	✓	アタック (Fraggle)	Enabled	All	All	All	All
QIBM_ICMP_Redirect	✓	アタック (ICMP Redirect)	Enabled	All	All	All	All
QIBM_IP_Fragment	✓	アタック (IP Fragment)	Enabled	All	All	All	All
QIBM_Malformed_Packet	✓	アタック (Malformed Packet)	Enabled	All	All	All	All
QIBM_Outbound_Raw	✓	アタック (Outbound Raw)	Enabled	All	All	All	All
QIBM_Perpetual_Echo	✓	アタック (Perpetual Echo)	Enabled	All	All	All	All

➢ これで、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。

解説：

・ここでは、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」を作成しています。

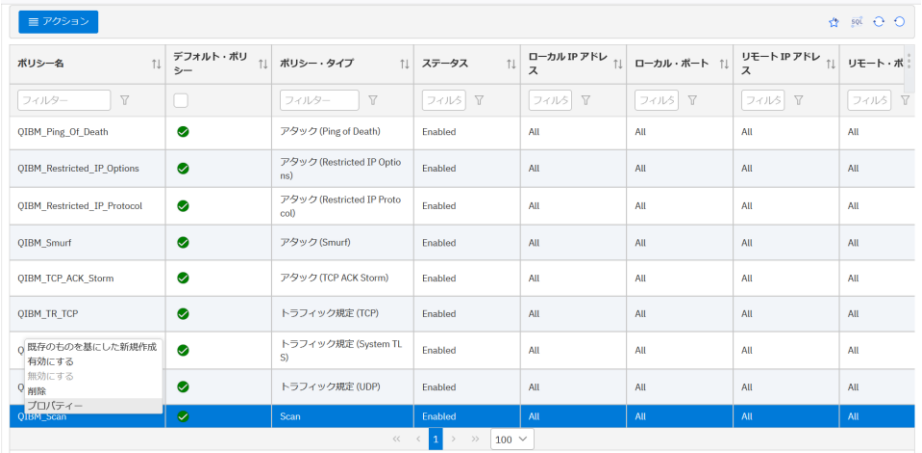
・デフォルトIDS ポリシーの多くのプロパティー設定は読み取り専用ですが、ユーザーが作成したIDS ポリシーのプロパティー設定はすべて編集可能です。

・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。

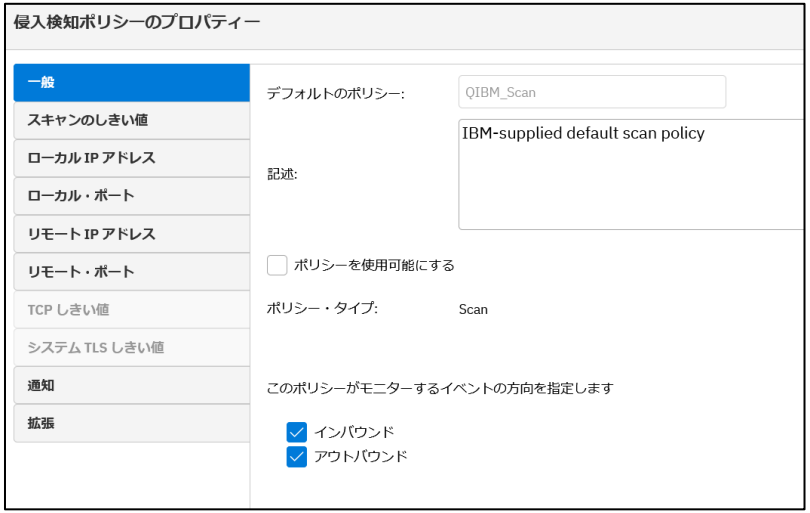
3. 侵入検知機能を使ってみよう

✓ 例として、「デフォルトの侵入検知ポリシー・セット」の「スキャン・ポリシー」の表示

⑥作成されたポリシーの一番下にある、「QIBM_Scan」を選択して、「プロパティ」を選択します。



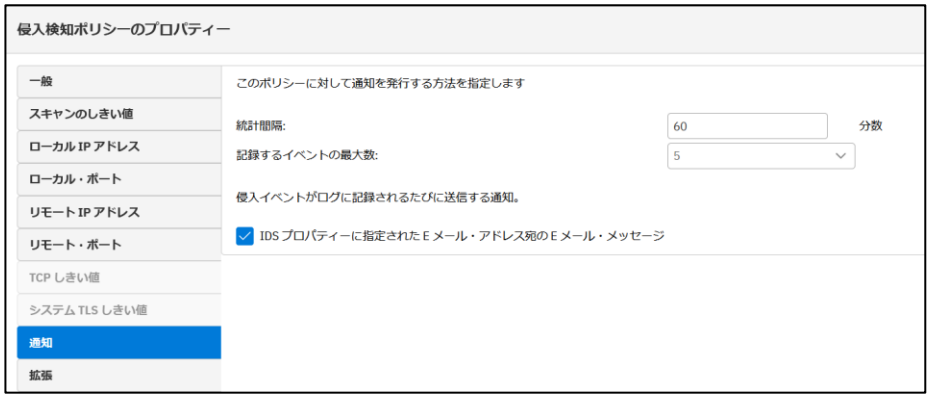
⑦下記のように表示されればOKです。



解説：

・デフォルトセットの「スキャン・ポリシー」の設定値は下記のようになっています。

- ✓ この IDS スキャン・ポリシーは、全てのローカル・IP及びポートとリモートIP・ポートの 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、120分間の間隔の中で低速スキャンの数が 10 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 5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。



3. 侵入検知機能を使ってみよう

（２）侵入検知の通知の宛先を設定と開始

①Navigator for iの「セキュリティ」
→「侵入検知」→「侵入検知の管理」を選択

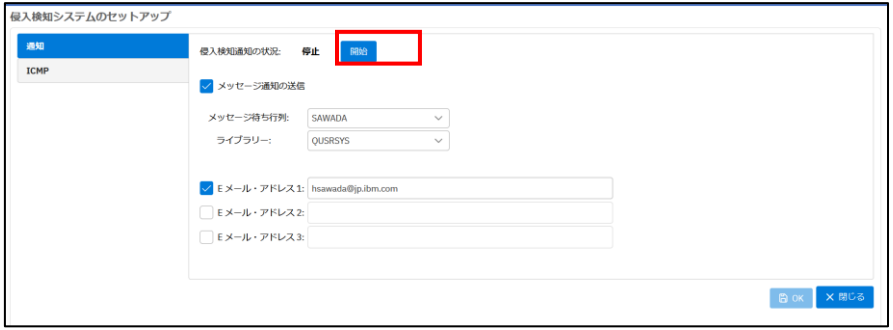
②通知メッセージを送る宛先を指定します。
・メッセージ待ち行列(デフォルトはQSYSOPRです)
例として、 SAWADA/QUSRSYSを指定
・E-MAILアドレスは任意です。
例として、hsawada@jp.ibm.comを指定

この後、「ICMP」のタブを選択します。

3. 侵入検知機能を使ってみよう

③ICMPリダイレクト・メッセージの許可は、
デフォルトのままでOKです。

④再度、「通知」タブに戻り、
この後、「開始」を選択します。
これで侵入検知機能が開始され、モニターされます。



解説：

・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待ち行列へのメッセージとして、および電子メールとして送信するように、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ることができるようにします。

・「ICMPリダイレクト・メッセージ」は、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。(TCP/IPの通信状況を確認する、Ping監視のプログラムです。)
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。

・IDS 通知を開始する前提とすて、監査システム値を *AUDLVL および *ATNEVT に設定する必要があります。下のコマンドを処理する必要があります。（侵入検知機能は、監査ジャーナルが起動していることが前提）

3. 侵入検知機能を使ってみよう

（3）スキャン・イベントの侵入検知のテスト

✓ 設定した侵入検知機能をテストするために、ポート・スキャンを実施

・WindowsPCから、ポートスキャン・ツール(ここではnmapツール)を使って、侵入検知を設定したIBM iマシンをスキャンの実施。

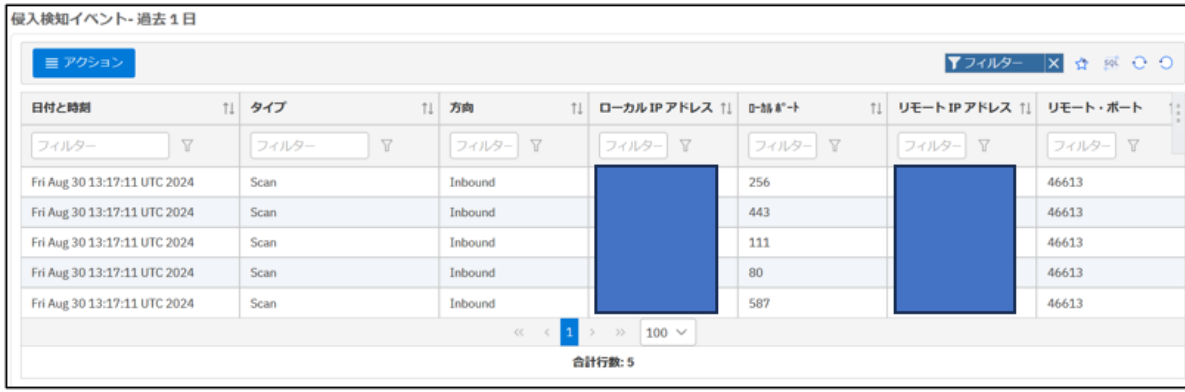
```
C:¥Users¥12345678>NMAP XXX.XXX.XXX.XXX
Starting Nmap 7.94 ( https://nmap.org ) at 2024-08-30 13:10 東京 (標準時)
Nmap scan report for XXX.XXX.ibm.com (XXX.XXX.XXX.XXX)
Host is up (0.031s latency).
Not shown: 982 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
25/tcp  open  smtp
.
.

2001/tcp open  dc
2002/tcp open  globe
2003/tcp open  finger
2004/tcp open  mailbox
2006/tcp open  invokator
2008/tcp open  conf
3000/tcp open  ppp

Nmap done: 1 IP address (1 host up) scanned in 1.26 seconds
```

3. 侵入検知機能を使ってみよう

（４）侵入検知のイベントの表示

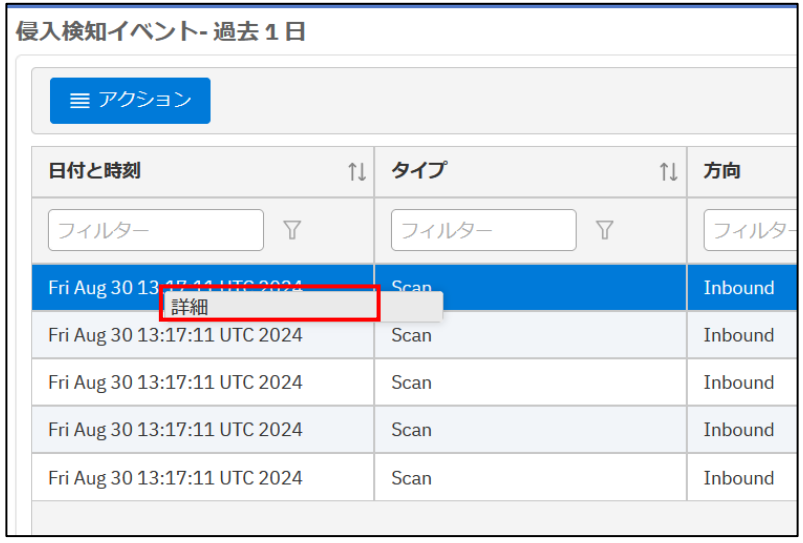
①Navigator for iの「セキュリティ」
→「侵入検知」→「イベントの表示」を選択

②下記のようにスキャン・イベントとして、記録されているのが表示される。
*ローカルIPとリモートIPは、隠しています。デフォルト・ポリシーで最大5件の記録に設定したので、下記の5件が表示されます。

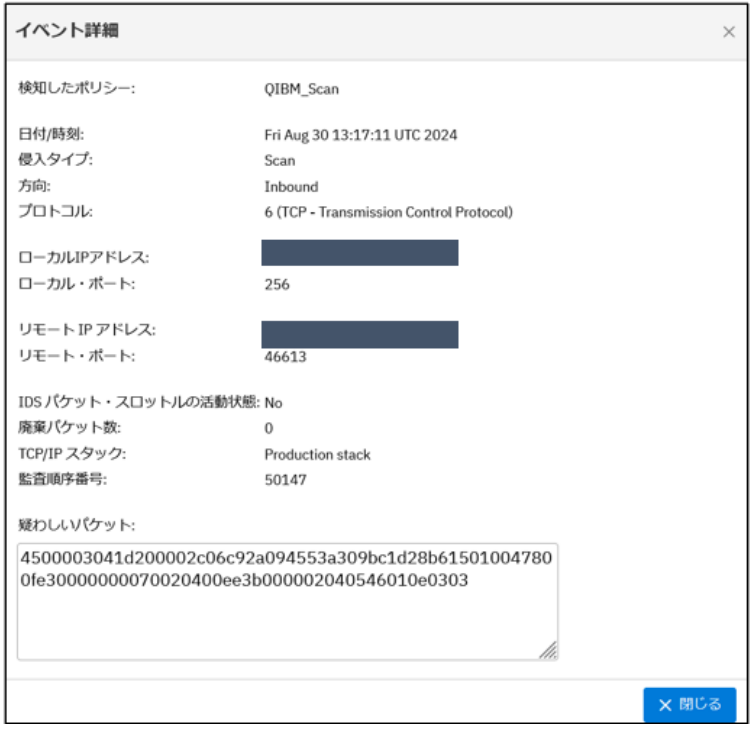


3. 侵入検知機能を使ってみよう

③一番上の行で、右クリックで、「詳細」を選択

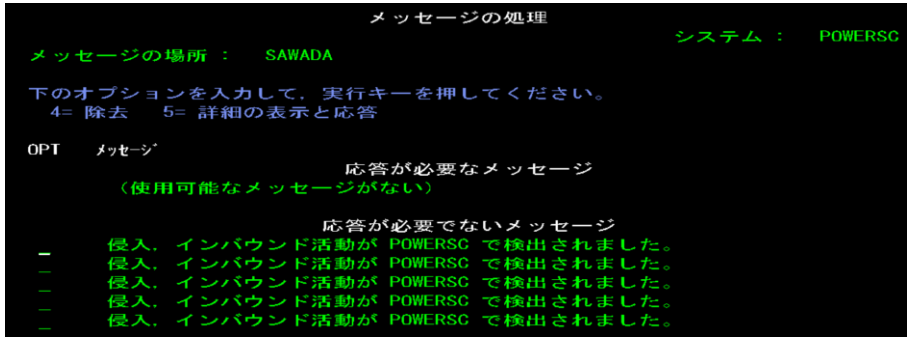


④下記ようにスキャン・イベントの詳細が記録されています。
- 侵入タイプはScan
- インバウンド（外部からの攻撃）として記録
- プロトコル番号6はtcp

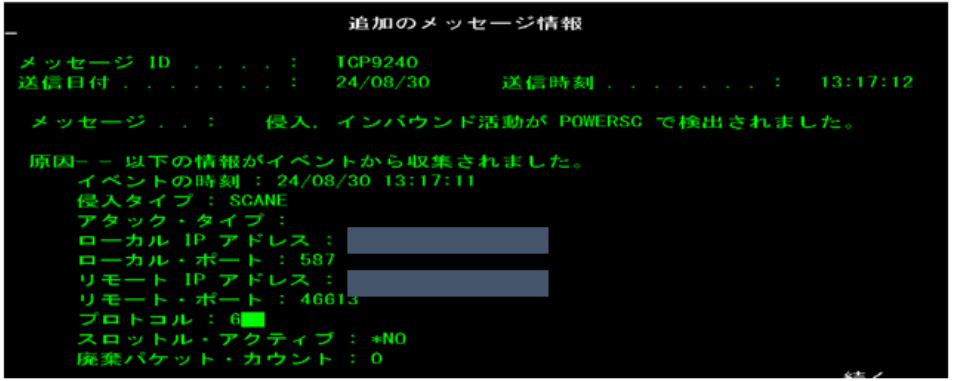


3. 侵入検知機能を使ってみよう

⑤侵入検知の設定で、MSGQ（SAWADA)に、通知されるように設定しました。確認してみます。
「DSPMSG SAWADA」コマンドで下記が表示されます。



⑥「5：詳細の表示」を入力して、詳細を表示してみます。
Navigator for iと同様のメッセージがリアルタイムに通知されているのが確認できました。



解説：

・侵入検知機能でスキャン・ポリシーを設定していると、個々のポートのスキャンを検知します。
統計データを収集して監査することにより、システムがグローバル・スキャンのターゲットとなっているかどうかを判断することができます。
TCP/IP スタックが侵入イベントを検知すると、スタックは侵入検知機能を呼び出し、統計および監査レコードを生成します。

・単一の送信元 IP が規定の期間内に複数の情報収集を行ったときにスキャンと認識されます。
スキャン・ポリシーは、トラフィックを拒絶することはありません。スキャン・イベントを検知して報告するだけです。

・このように「デフォルト侵入検知ポリシー・セット」を設定していると、簡単に、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ことができます。

まとめ：侵入検知機能を使ってみよう

- ✓ **外部からの攻撃の検知には、侵入検知機能が利用できます。**
- ✓ **IBM i の最新のHTTP サーバーのPTFを適用すれば、IBM Navigator for iの侵入検知のメニューから操作が可能です。**
- ✓ **監査ジャーナルを、設定・始動していれば、デフォルトの「侵入検知ポリシーセット」を使って、すべてのタイプのイベントの検知を簡単に設定できます。**

侵入検知機能を活用して、外部からの脅威に備えましょう。

4. 補足情報

1. IBM i の侵入検知（マニュアル）
   https://www.ibm.com/docs/ja/i/7.5?topic=security-intrusion-detection

2. システム・セキュリティーの計画と設定
   https://www.ibm.com/docs/ja/ssw_ibm_i_75/pdf/rzamvpdf.pdf

3. IM (侵入モニター) ジャーナル項目
   https://www.ibm.com/docs/ja/i/7.5?topic=entries-im-intrusion-monitor-journal

4. 侵入検知スキャン・ポリシーの例
   https://www.ibm.com/docs/ja/i/7.5?topic=detection-example-intrusion-scan-policy

IBM i 関連情報

IBM i ポータル・サイト
https://ibm.biz/ibmijapan

i Magazine (IBM i 専門誌。春夏秋冬の年4回発刊)
https://www.imagazine.co.jp/IBMi/

IBM i World 2023 オンデマンド・セミナー
https://ibm.biz/ibmiworld2023

IBM i World 2022 オンデマンド・セミナー
https://video.ibm.com/recorded/132423205

月イチIBM Power情報セミナー「IBM Power Salon」
https://ibm.biz/power-salon

IBM i 関連セミナー・イベント
https://ibm.biz/powerevents-j

IBM i Club (日本のIBM i ユーザー様のコミュニティー)
https://ibm.biz/ibmiclubjapan

IBM i 研修サービス (i-ラーニング社提供)
https://www.i-learning.jp/service/it/iseries.html

IBM Power Systems Virtual Server 情報
https://ibm.biz/pvsjapan

IBM i 情報サイト iWorld
https://ibm.biz/iworldweb

IBM i サポートロードマップ
https://www.ibm.com/downloads/cas/JB8AXO9V

IBM i 7.5 技術資料
https://www.ibm.com/docs/ja/i/7.5

IBM Power ソフトウェアのダウンロードサイト (ESS)
https://ibm.biz/powerdownload

Fix Central (HW・SWのFix情報提供)
https://www.ibm.com/support/fixcentral/

IBM My Notifications (IBM IDの登録 [無償] が必要)
「IBM i」「9009-41G」などPTF情報の必要な製品を選択して登録できます。
https://www.ibm.com/support/mynotifications

IBM i 各バージョンのライフサイクル
https://www.ibm.com/support/pages/release-life-cycle

IBM i 以外のSWのライフサイクル (個別検索)
https://www.ibm.com/support/pages/lifecycle/

IBM i Advantage 2024 開催決定!

12月3日(火)・4日(水)
IBM虎ノ門イノベーションスタジオ (メイン会場)
IBM大阪中之島フェスティバルタワー・ウエスト (中継)

12月24日(火)
Webセミナー + Q&Aセッション

今から**カレンダーブロック**をお願いいたします。
下記サイトに最新情報を掲載します↓

https://ibm.biz/ibm-power-user-**community**

IBM i
continuous innovation
continuous integration
Advantage 2024