2006 年 4 月（第 1 版）

Cisco Security Device Manager サンプル設定ガイド

SDM 2.1.2 2005/09 リリース版

Cisco IOS IPS 設定

I 概　要

Cisco IOS Intrusion Prevention System（IPS）機能は、Cisco IOS Software ベースのルータ上で実現される詳細なパケット検査のためのインライン シグニチャベースのソリューションです。

Cisco IOS IPS は Cisco SDM から GUI で操作することができます。IPS シグニチャは Cisco ルータに動的にロードされ、シグニチャによって識別された攻撃について、Cisco IOS IPS がアラームの送信、接続のリセット、パケットドロップなどのどのような処理を行うかをカスタマイズすることができます。

シスコ SDM では、ルータのインターフェイスで IPS を有効にすること、cisco.com からダウンロードされたシグニチャ定義ファイル（SDF）をルータに導入すること、IPS シグニチャ チューニングの結果カスタマイズされたシグニチャをルータに導入することができます。また警告メッセージを syslog サーバに送信するよう指定したり、またセキュリティイベントを報告するために Security Device Event Exchange（SDEE）プロトコルを使用するようにルータを構成することができます。

本設定ガイドでは、初めての IPS 導入のために次のステップをカバーしています。

(1) IPS の有効化

(2) SDF を用いた IPS のアップデート

(3) IPS シグニチャのチューニング

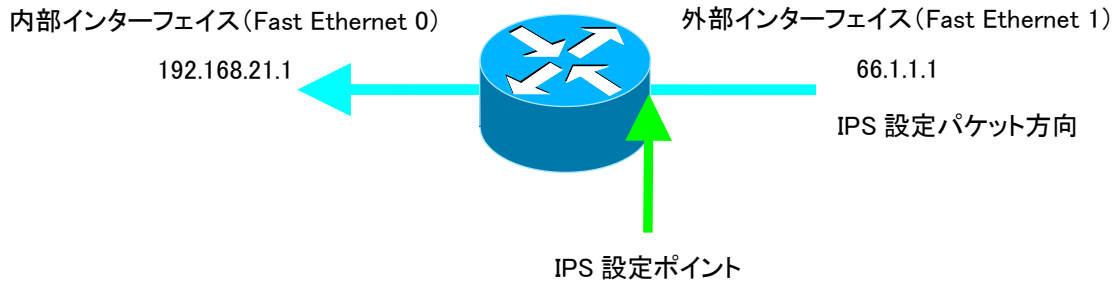
II 設 定 手 順

まずは、Cisco 推奨の 3 つのシグニチャファイル(attack-drop.sdf、128 MB.sdf、256 MB.sdf)は Cisco SDM に含まれており、ルータのメモリ構成にあわせ、3 つの中で最適なシグニチャファイルをフラッシュ メモリにロードします。また最新の SDF を cisco.com(http://www.cisco.com/cgi-bin/tablebuild.pl/ios-sigup)から手動でダウンロードし、ローカルワークステーションに保存しておくこともできます。Cisco IOS Software のセキュリティコマンドの参照に関しては http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123tcr/123tsr/sec_01gt.pdf を参照してください。

1. IPS の有効化

ここでは、Cisco SDM IPS ウィザードを実行し、WAN インターフェイスで IPS を有効にした後にルータへ SDF をインポートします。この例では、Fast Ehtnernet 0 が内部インターフェイス、Fast Ethernet 1 が外部インターフェイスとして構成されたルータ(機種は Cisco 1812-J)において、IPS を外部インターフェイスに受信されるトラフィックに対して適用します。

(システム構成)



SDM の構成モードで侵入防止を選択し、[IPS の起動]（図 1）をクリックします。SDEE が有効になっていない場合、図 2 のメッセージが表示されます。「OK」をクリックすると SDM がルータ上で SDEE を有効化し、IPS ホーム画面（図 3）が表示されます。

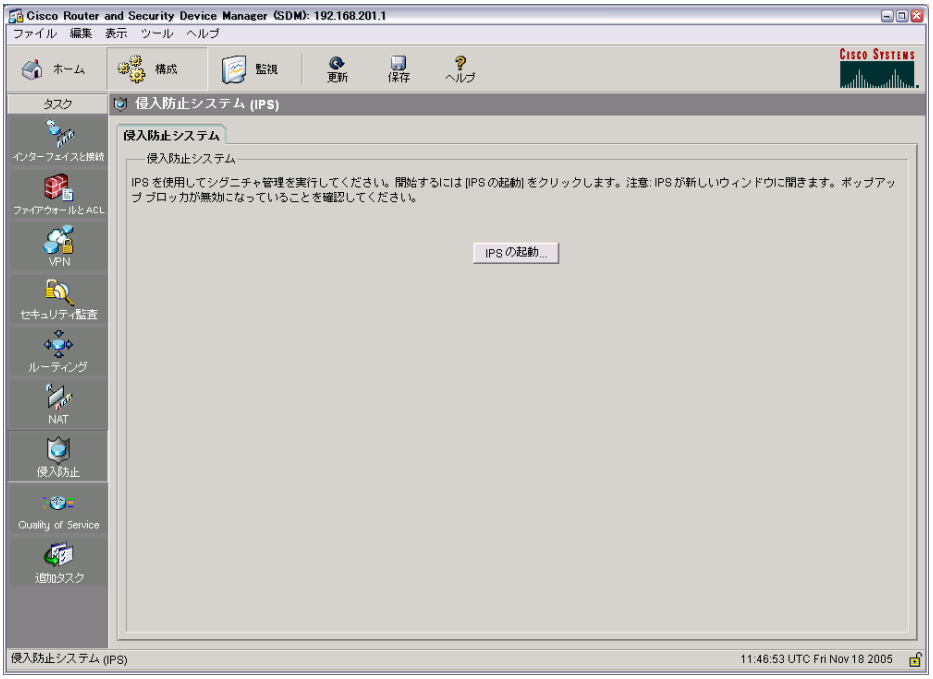


図 1：侵入防止起動画面

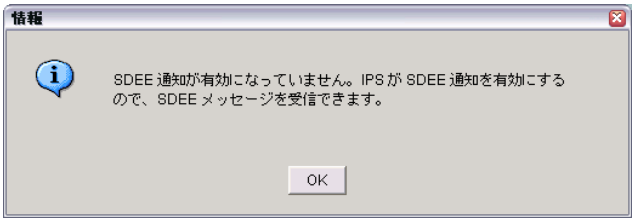


図 2：SDEE 有効化の通知

図 3:IPS ホーム

起動したばかりの IPS は何も定義がされておらず、機能していません。IPS 構成画面（図 4）において、外部インターフェイスである Fast Ethernet 1 を選択し、「有効」をクリックして IPS インターフェイスに適用します。

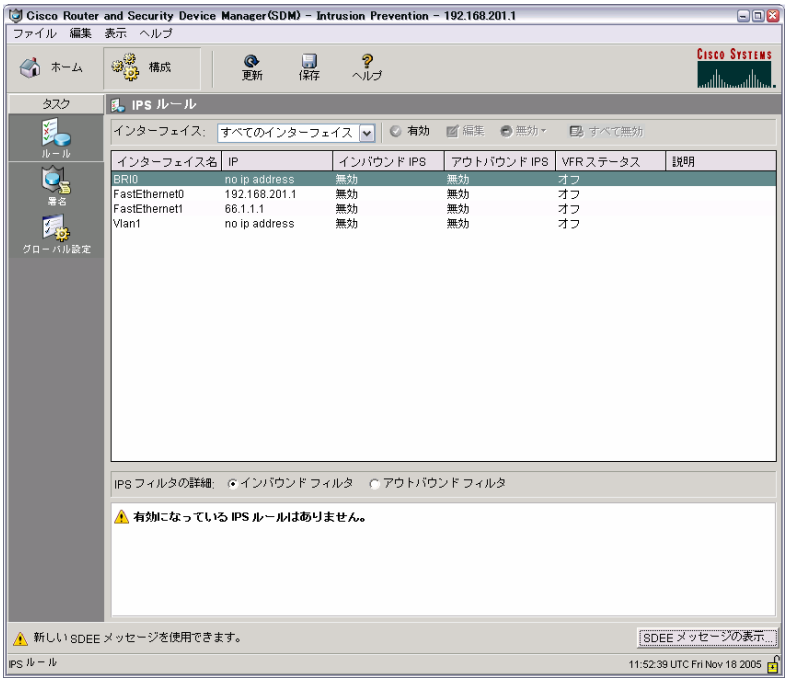


図 4:IPS 構成画面

ルータのフラッシュ メモリにあらかじめ SDF がインストールされていると、図 5 のようにルータがファイルを検出し確認メッセージが表示されます。「はい」をクリックします。フラッシュ メモリ内に利用できる SDF が存在しない場合には、SDM は登録されているビルトインシグニチャ（＝IOS が搭載しているシグネチャ）を利用して IPS を構成します。

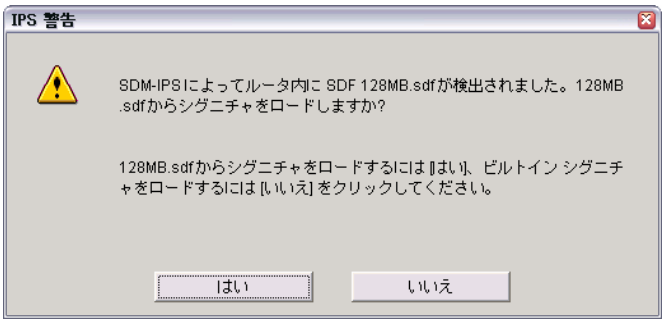


図 5：SDF の検出

「インターフェイスに対して IPS を有効にする」画面（図 6）では、指定した Fast Ethernet 1 インターフェイスに対するインバウンド（受信側）のパケット検査を指定し、「OK」をクリックします。（図 7）。IPS で検査をしたくないトラフィックは、それを識別するアクセスリストを図 6 のインバウンドフィルタに入力してから「OK」をクリックします。

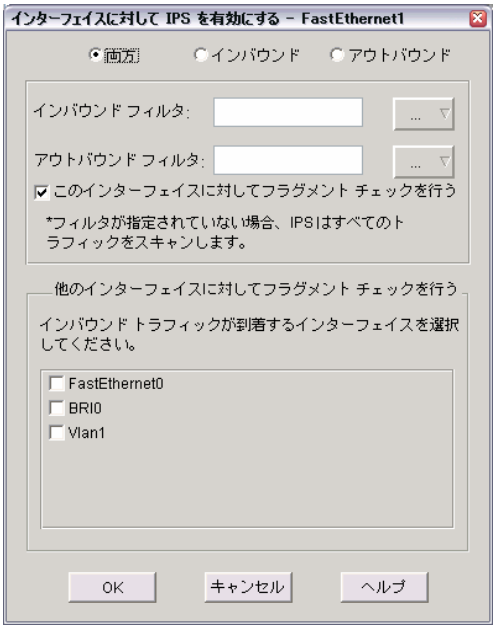


図 6：インターフェイスに対する IPS 設定（1）

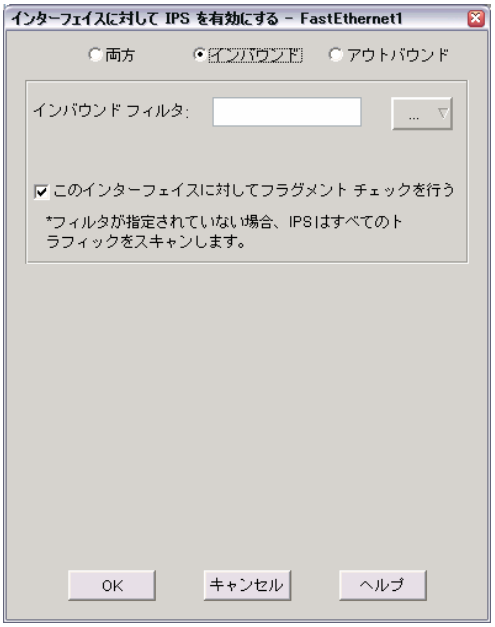


図 7:インターフェイスに対する IPS 設定(2)

「インターフェイスに対して IPS を有効にする」設定画面で OK をクリックすると、SDM が受信した SDEE メッセージが表示(図 8)されます。SDEE メッセージは、IPS の変更を行うと出力されます。処理を進めるには「閉じる」をクリックします。

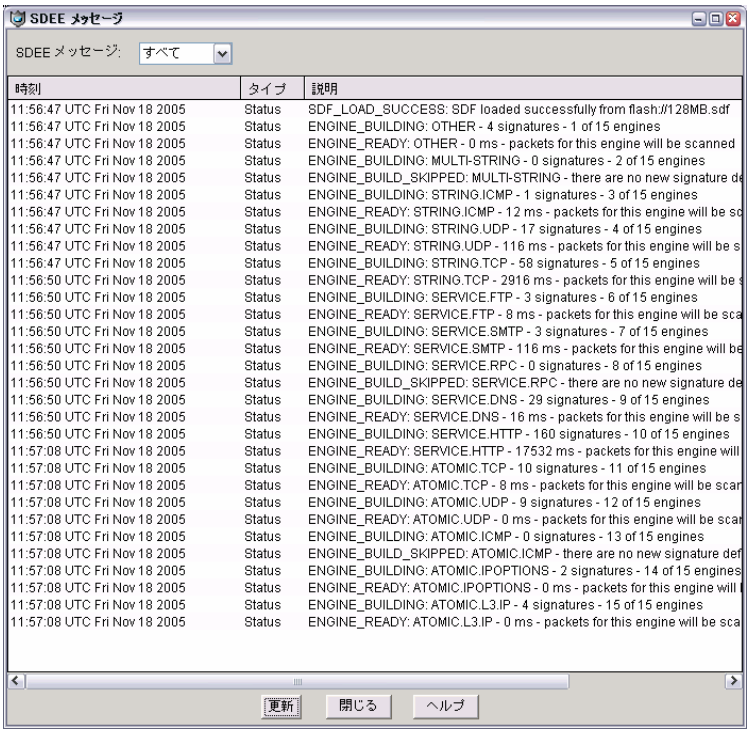


図 8:SDEE メッセージ

この例では、IPS を外部インターフェイスに受信されるトラフィックに関して言及していますが、アウトバウンドのパケット検査やアウトバウンド フィルタの適用が必要な場合（例　アウトバウンドWANトラフィックで社内に留まるものは IPS 対象外とし、インターネットに出て行くものは IPS 検査する等）、「インターフェイスに対して IPS を有効にする」画面（図 6）から同様に設定が可能です。

処理が完了すると、IPS ルール画面で Fast Ethertnet 1 のインバウンド IPS が有効になっていることが確認できます（図 9）。

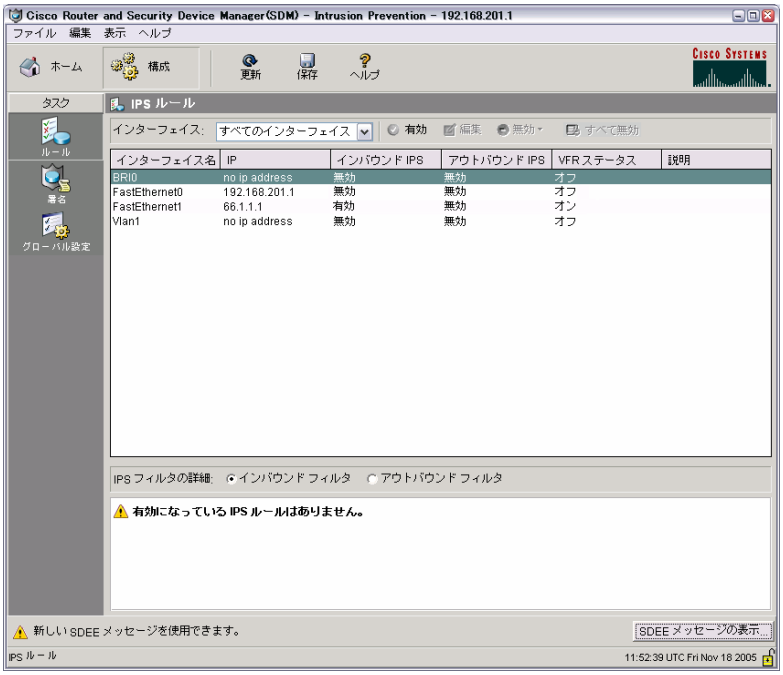


図 9：インターフェイス Fast Ethernet 1 への IPS 有効化

またインターフェイスに対する IPS の設定が完了すると、「署名」タスクに SDF またはビルトインシグニチャからロードされたシグニチャが表示されます（図 10）。

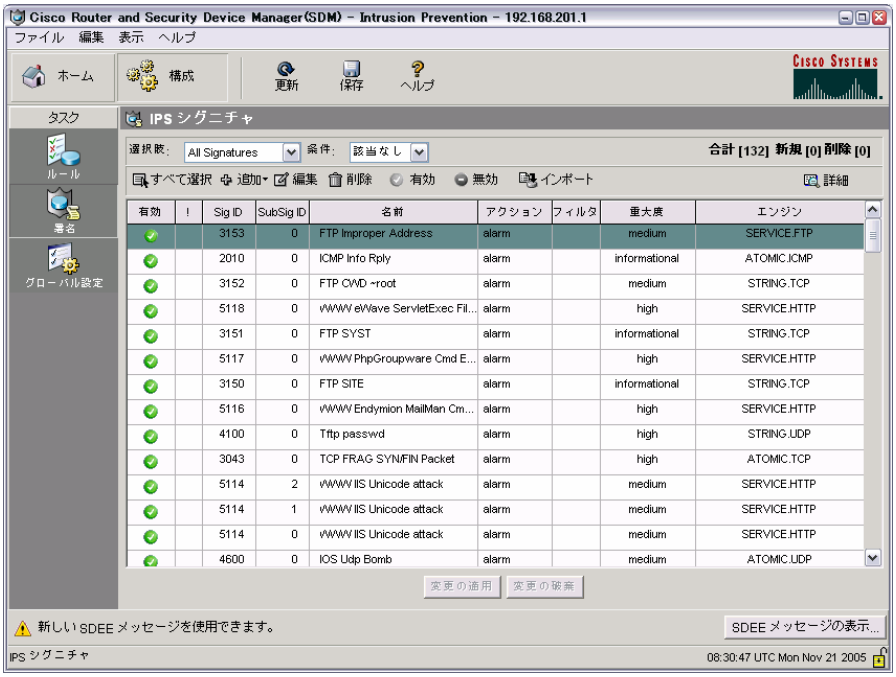


図 10：IPS シグニチャ

（注意）デフォルトでは全シグネチャが有効です。必要に併せ、使わないシグニチャを無効にしたり、シグニチャの各パラメータを変えたりして調整を行ってください。

2. シグニチャのインポート

更新された SDF などからシグニチャをインポートしてカスタマイズするには、IPS シグニチャ画面で「インポート」クリックします。インポート元のファイル選択ウィンドウが開き、SDF を保存しているファイルを指定して「開く」をクリックします（図 11）。

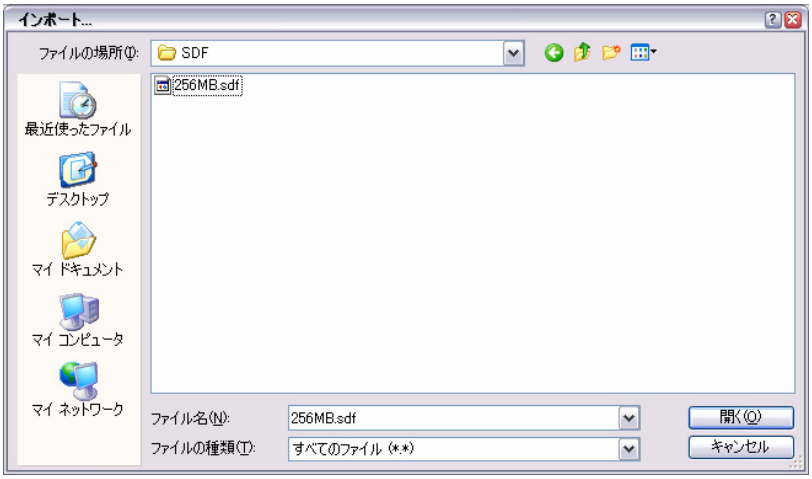


図 11：インポート元ファイルの指定

インポートする SDF を開くと、その SDF でサポートされているシグニチャの一覧が表示されます（図 12）。すでにロードされているシグニチャは灰色に表示され、ロードされていないシグニチャは黒く表示されています。この例では、これらのシグニチャから「IOS HTTP Unauth Command Execution（ID：5129）」をインポートします。

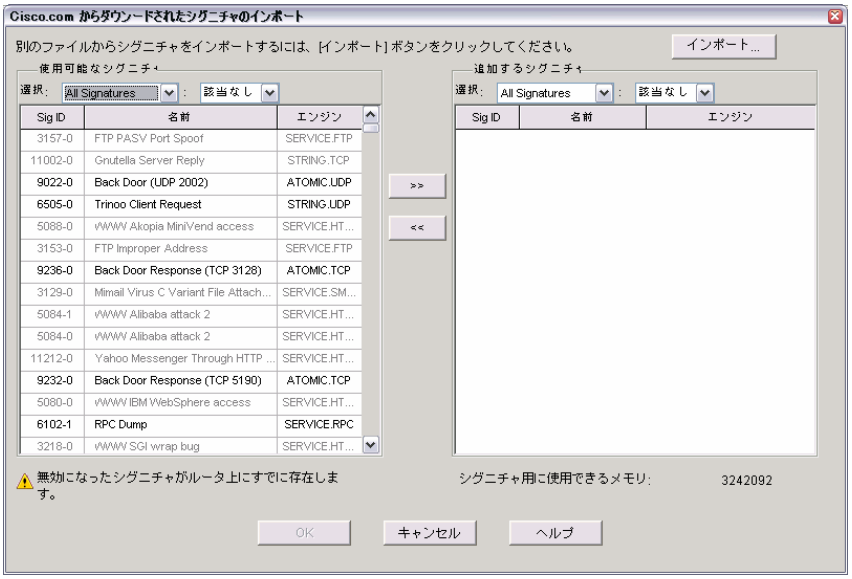


図 12：インポート元のシグニチャ

選択欄から「OS」、「IOS」を選択すると、選択したカテゴリに適合するシグニチャに絞り込まれます（図 13）。この中から「IOS HTTP Unauth Command Execution（ID：5129）」を選択し、追加ボタン（ >> ）をクリックして追加するシグニチャ欄に追加します。

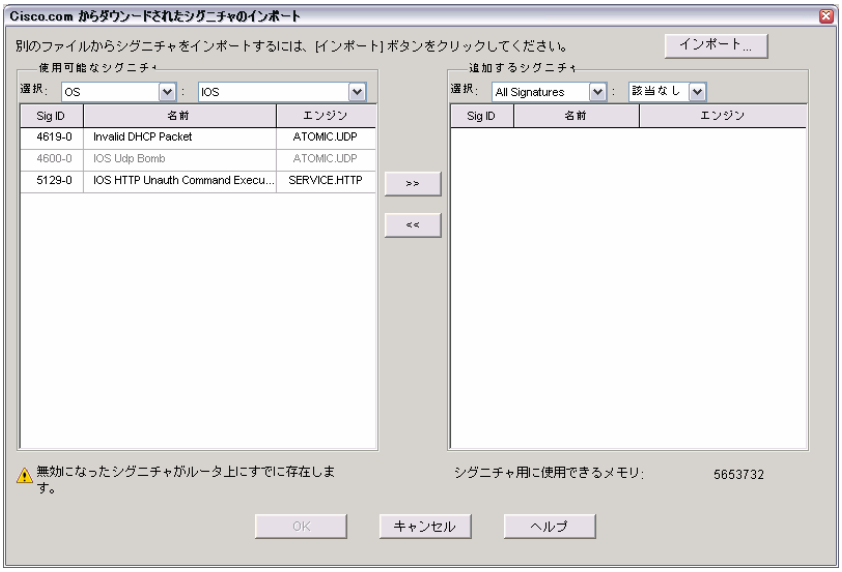


図 13：シグニチャの絞込み

「IOS HTTP Unauth Command Execution（ID：5129）」が追加するシグニチャに表示されたら、「OK」をクリックします（図 14）。

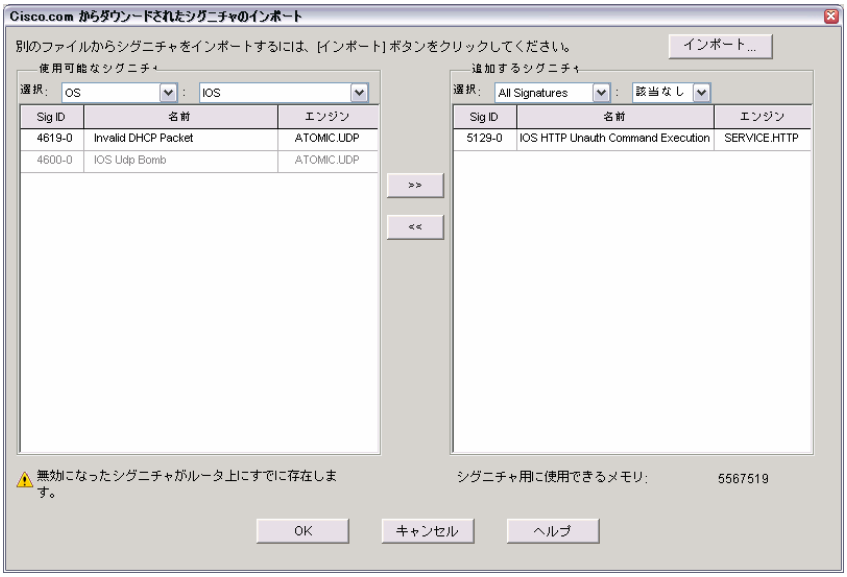


図 14：追加するシグニチャの決定

選択したシグニチャが SDM 上にロードされ、変更フラグ( )が表示されます(図 15)。この段階ではまだルータへ反映されていません。ルータへの反映を行う場合には「変更の適用」を、取り消すには「変更の破棄」をクリックします。

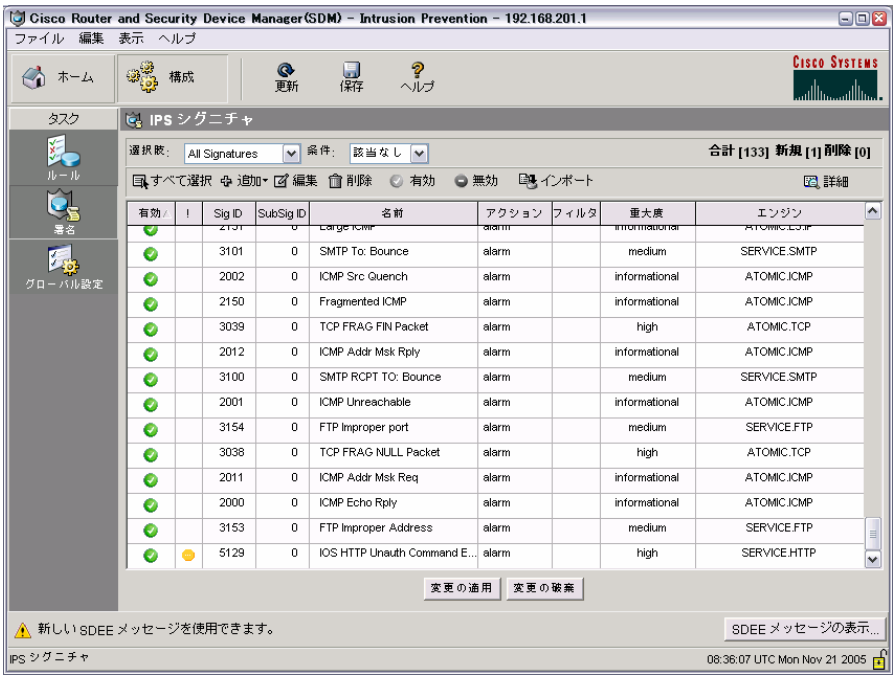


図 15:シグニチャの追加

ルータの構成内容と SDM の構成内容が同期されると、「変更の適用」及び「変更の破棄」ボタンがグレーアウトして選択できなくなります(図 16)。

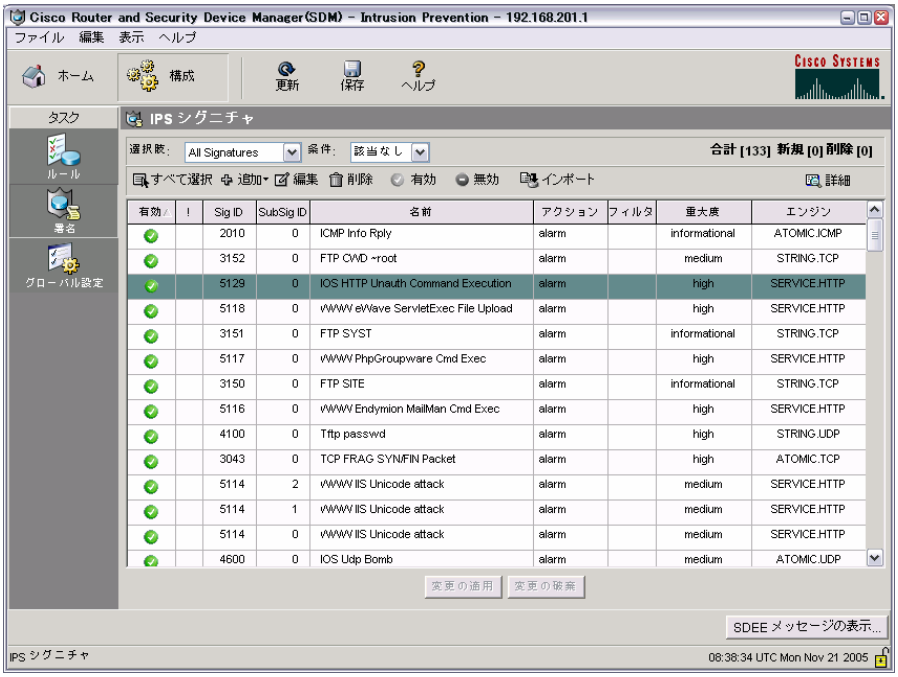


図 16:シグニチャ追加の完了

3. シグニチャの編集

シグネチャの編集には二通りの方法があります。一つは「編集」をクリックしてシグニチャの編集ウィンドウから変更するもの、もう一つは対象のシグニチャを右クリックして表示されるメニューから選択するものです。まず、シグニチャの編集ウィンドウを使用した編集方法を説明します。

ここでは「ID:1102　Impossible IP Packet」のアクションを Alerm から Drop へ変更します。広範なシグニチャの中から目的のシグニチャを探すのは困難ですが、各列の項目名をクリックして項目名毎の昇順/降順で並べ替えを行ったり、また選択肢リストボックスで大分類を、さらにその大分類から中分類を絞り込むことでシグニチャ検索に要する負担を軽減することができます(図 17)。

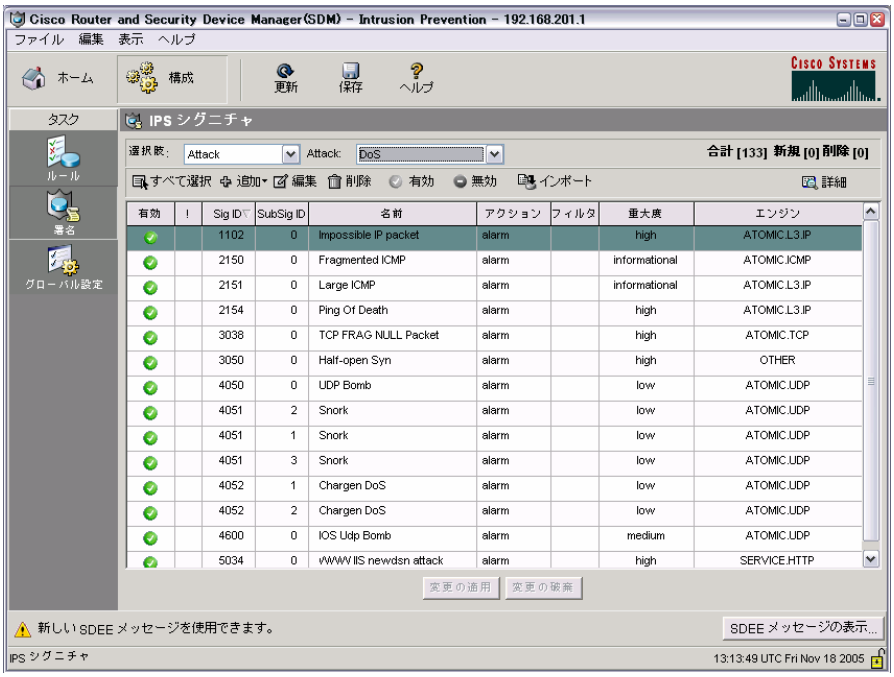


図 17:編集対象シグニチャの絞込み

目的のシグニチャが特定できたら、そのシグニチャを選択して「編集」をクリックし、シグニチャの編集ウィンドウを開きます（図 18）。

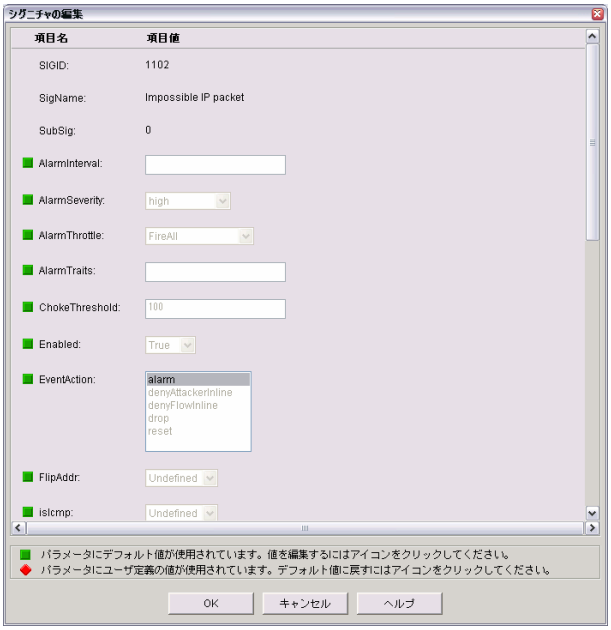


図 18：シグニチャ編集ウィンドウ

シグニチャの編集ウィンドウでは、値がデフォルト設定のパラメータにはアイコン「■」が、ユーザ定義のパラメータにはアイコン「◆」が表示されます。各パラメータの値を変更するには、これらのアイコンをクリックします。

パラメータ「EventAciton」のアイコンをクリックし、「drop」を選択します。また、パラメータ「AlarmThrottle」のアイコンをクリックし、「GlobalSummarize」を選択し、「OK」をクリックします（図 19）。

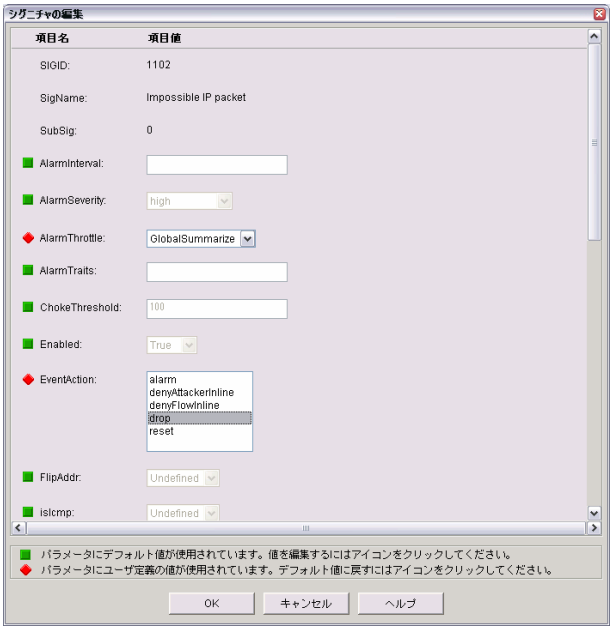


図 19：シグニチャパラメータの変更

選択したシグニチャの変更が SDM に反映され、変更されたシグニチャには変更フラグ( )が表示されます(図 20)。この段階では、変更内容はまだルータへ反映されていません。ルータへの反映を行う場合には「変更の適用」を、取り消すには「変更の破棄」をクリックします。

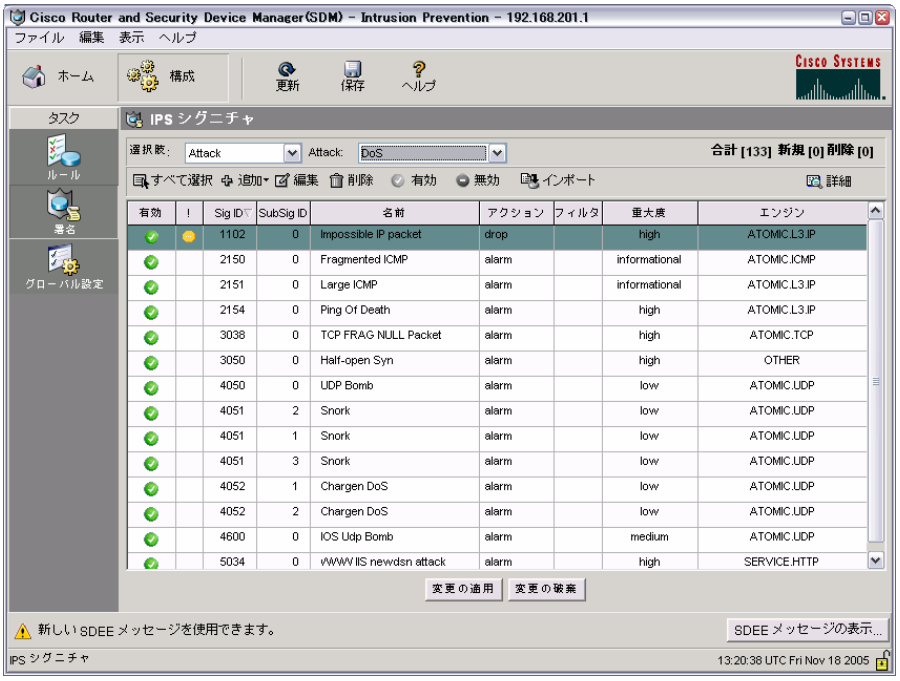


図 20:シグニチャ編集結果

変更の適用をクリックすると、シグニチャの変更内容がルータへ反映されます。ルータの構成内容と SDM の構成内容が同期されると、「変更の適用」及び「変更の破棄」ボタンがグレーアウトして選択できなくなります(図 21)。

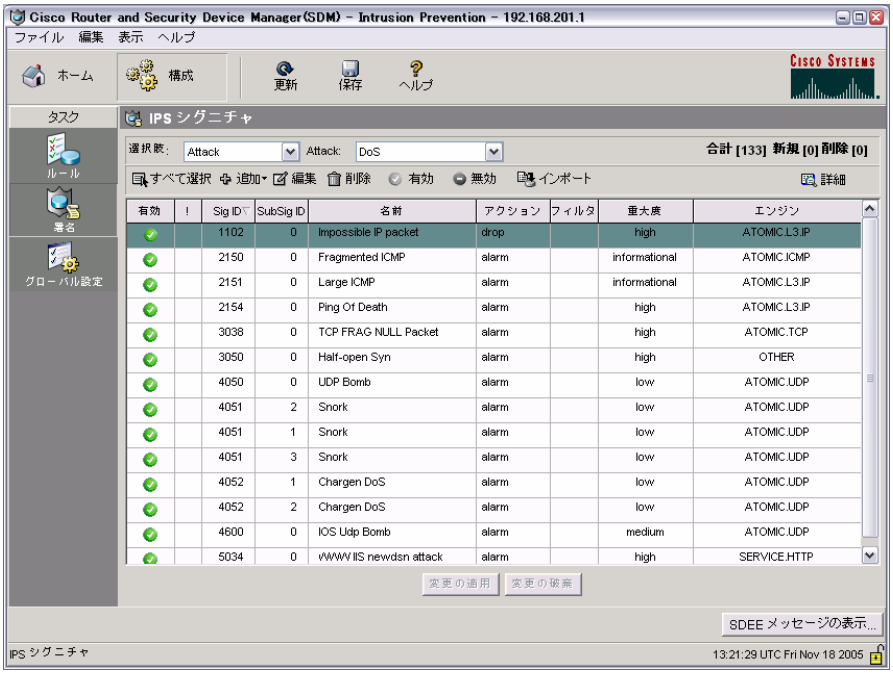


図 21:シグニチャ編集の完了

4. 画面からの変更

次の例では、「ID:3100 SMTP RCPT TO: Bounce」の重大度を Medium から Low に変更します。IPS シグニチャ画面で、選択肢「Service」、Service「SMTP」を選択します。Sig ID 欄をクリックすると、ID 番号順に昇順/降順で並べ替えを行うことができます(図 22)。

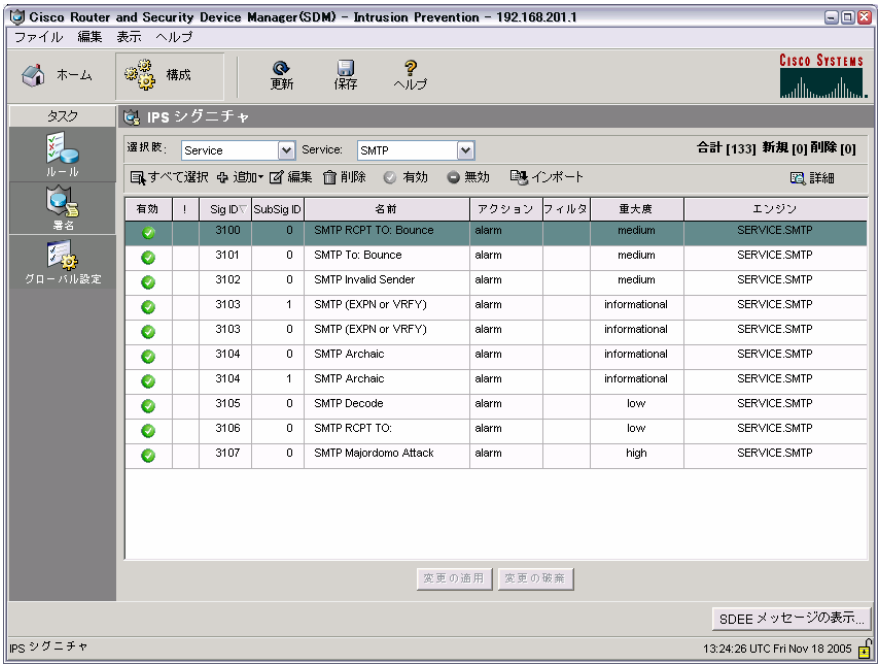


図 22:対象シグニチャの絞込み

Sig ID 3100 を選択し、右クリックしてメニューを表示させます。表示されたメニューから、「重大度の設定先」の「low」を選択します（図 23）。

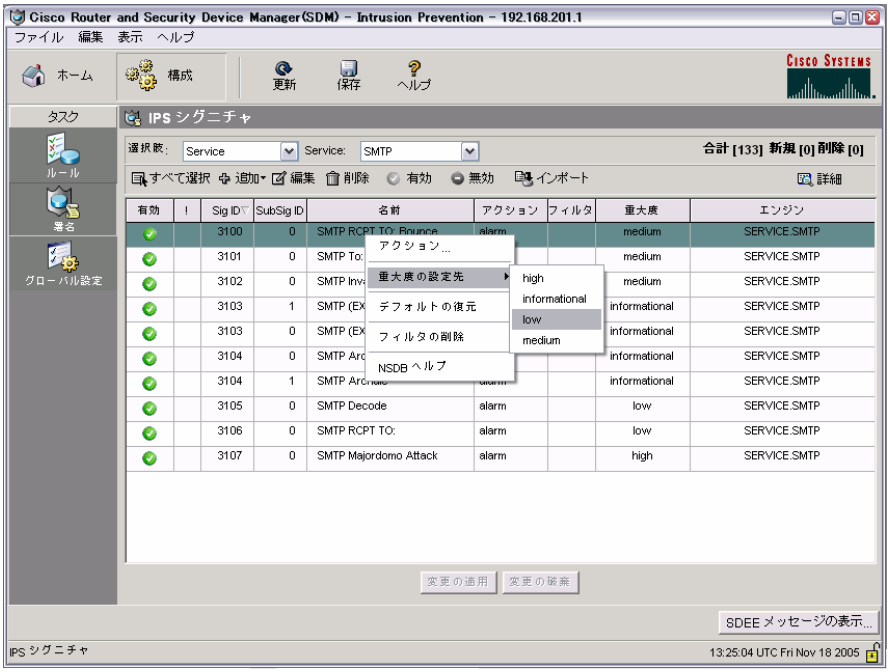


図 23：右クリックメニューからの編集

シグニチャの変更が SDM に反映され、変更されたシグニチャには変更フラグ（🟡）が表示されます（図 24）。この段階では、変更内容はまだルータへ反映されていません。ルータへの反映を行う場合には「変更の適用」を、取り消すには「変更の破棄」をクリックします。

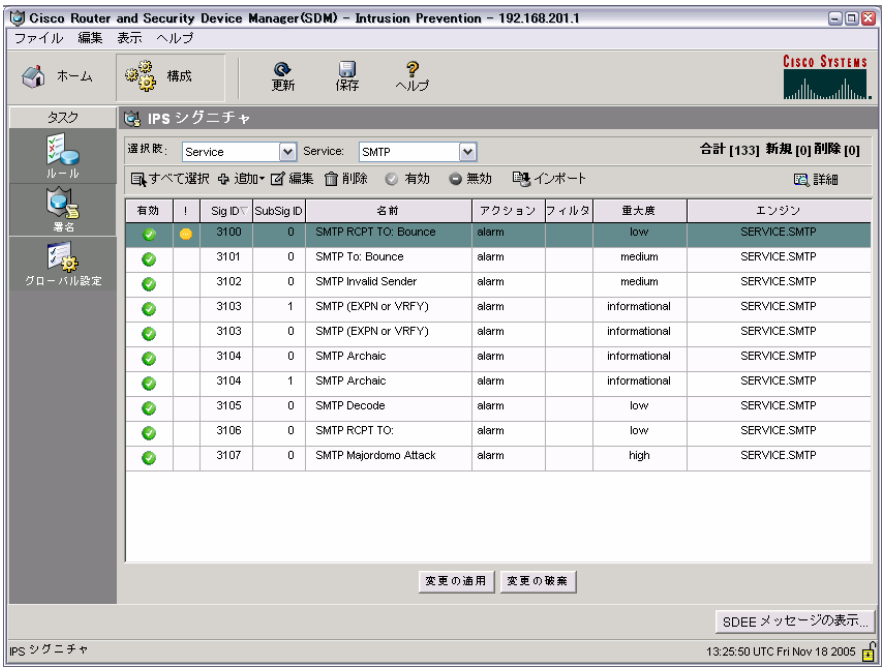


図 24：シグニチャ編集の完了

変更の適用をクリックすると、シグニチャの変更内容がルータへ反映されます。ルータの構成内容と SDM の構成内容が同期されると、「変更の適用」及び「変更の破棄」ボタンがグレーアウトして選択できなくなります（図 25）。

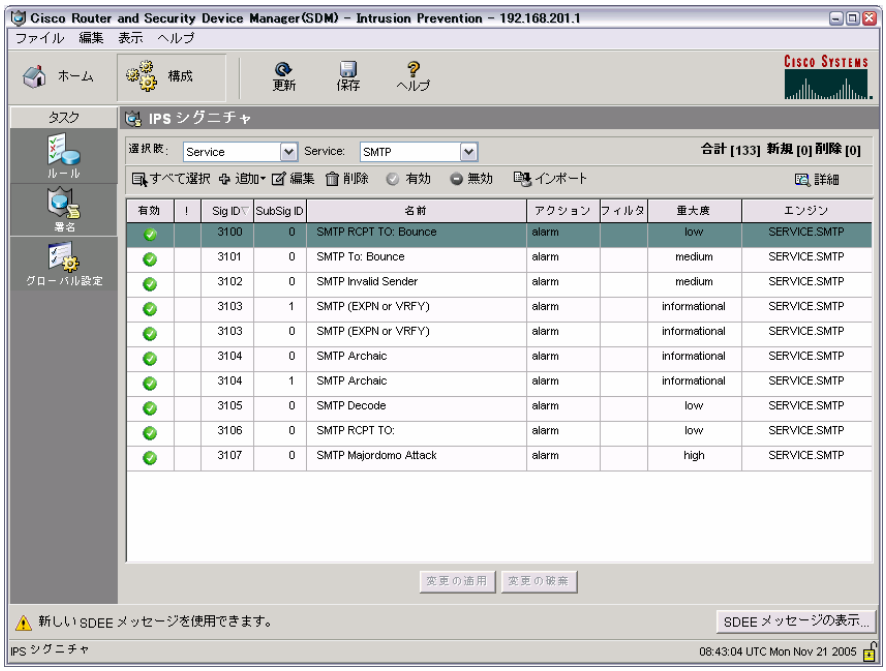


図 25：シグニチャ編集の反映

5. IPS グローバル設定

SDM のデフォルト設定では、シグニチャの変更に伴い、シグニチャ ソースファイルとしてルータのフラッシュ メモリに新しい SDF、sdmips.sdf を作成します。SDF 保存場所など、IPS 全体の設定を確認するには「グローバル設定」を参照します（図 26）。

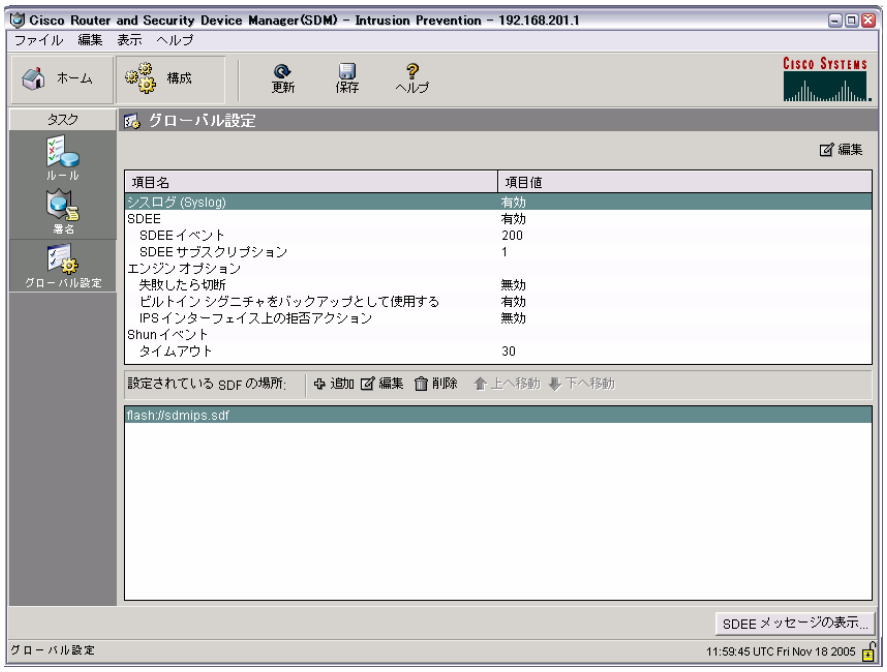


図 26：グローバル設定

またグローバル設定では、「編集」をクリックすることで syslog 通知、SDEE パラメータの編集、エンジンのオプションなどの設定を行うことができます（図 27）。

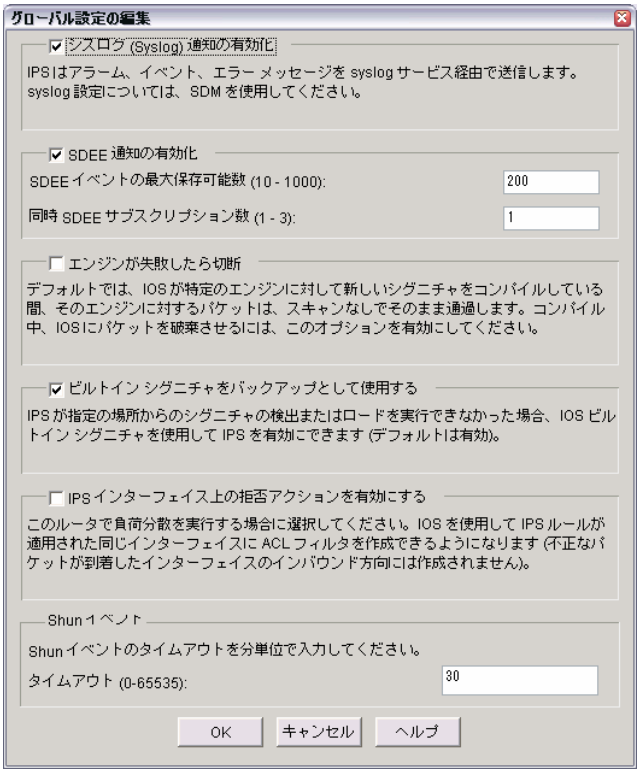


図 27：グローバル設定の編集

以上のように、SDM を用いると、Cisco IPS の有効化、確認そして各種チューニングが簡単に、そして迅速に行うことができます。

Cisco Security Device Manger サンプル設定ガイド
Cisco IOS IPS 設定

発行　　2006 年 4 月　第 1 版

発行　　シスコシステムズ株式会社