Chakra-WebSAM System Navigator
監視連携設定手順書

日本電気株式会社
第一システムソフトウェア事業部
2008年4月15日

目次

© NEC Corporation 2008

1．はじめに

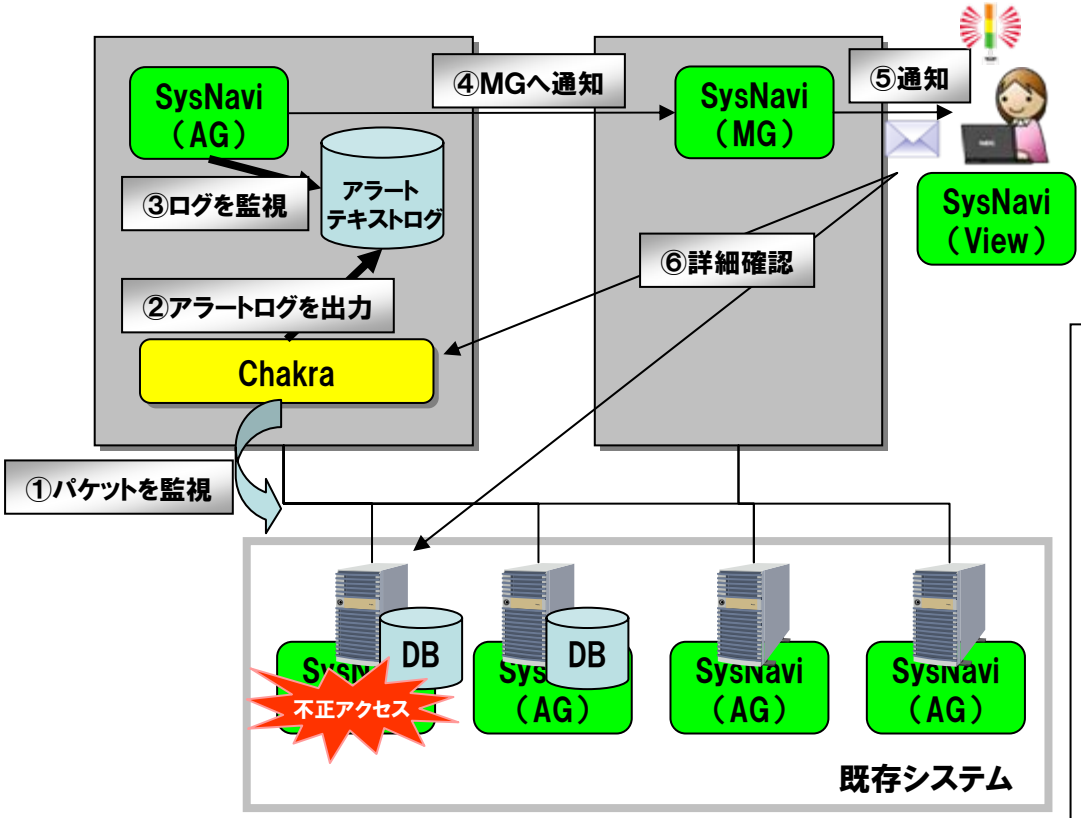
本書は、ニューシステムテクノロジーの「Chakra」とWebSAM System Navigatorの監視連携手順書です。

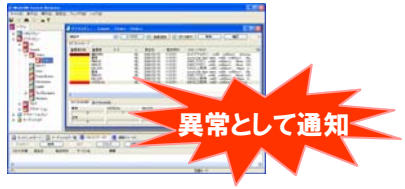
連携設定を行うことにより、Chakraでアラートが発生した際に、WebSAM System Navigator の監視端末で、そのアラートの内容を確認することができるようになります。

© NEC Corporation 2008

2. Chakra-WebSAM System Navigator連携による通報の流れ

Chakra-WebSAM System Navigator連携は、アプリケーションログ連携を実施。
上記の連携により、テンプレート利用で簡単導入＆運用を実現。





■処理の流れ

①Chakraがパケットを監視し不正パケットを検出
②Chakraが不正パケット検出をアラートテキストログに
　吐出す。
③SysNavi（AG）がテキストログを監視し、
　キーワードマッチングしたものを検出する。
④SysNavi（AG）が異常を検知するとSysNavi（MG）へ通知
⑤SysNavi（MG）から管理者へ通知を行う。
　（メール、パトライト、コンソール表示など）
⑥管理者はSysNavi（View）で初動を確認し、詳細は
　ChakraやDBへアクセスして確認する。

※SysNavi：WebSAM System Navigato
　AG：エージェント、MG：マネージャ、View：管理コンソール

© NEC Corporation 2008

3. WebSAM System Navigatorの初期設定

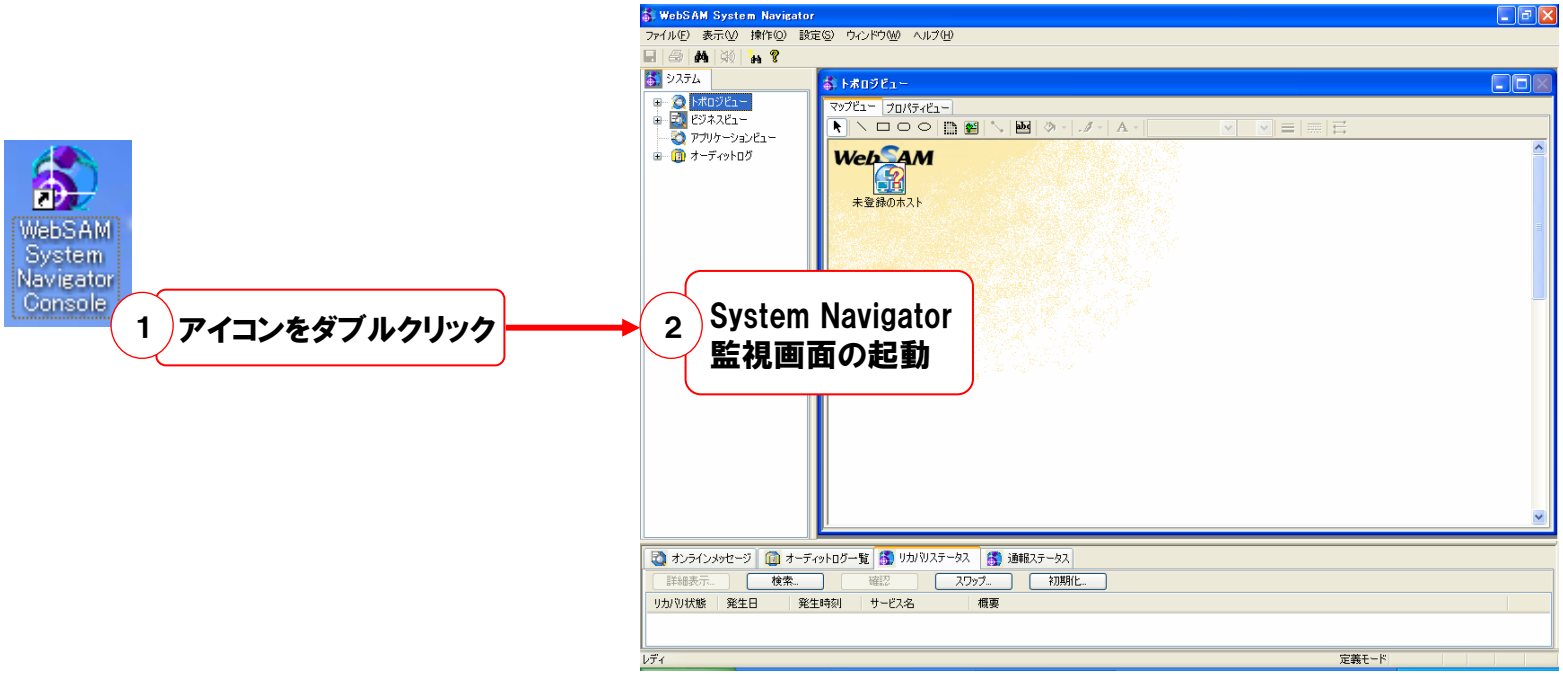
WebSAM System Navigator起動後の初期設定を行います。

初期状態では、WebSAM System Navigatorをインストールしたサーバ名が「不明のホスト」階層下に置かれてしまい、監視できないため、「不明のホスト」階層下より、通常階層へ移動することにより、監視できる状態にします。

© NEC Corporation 2008

3．1 WebSAM System Navigatorの起動

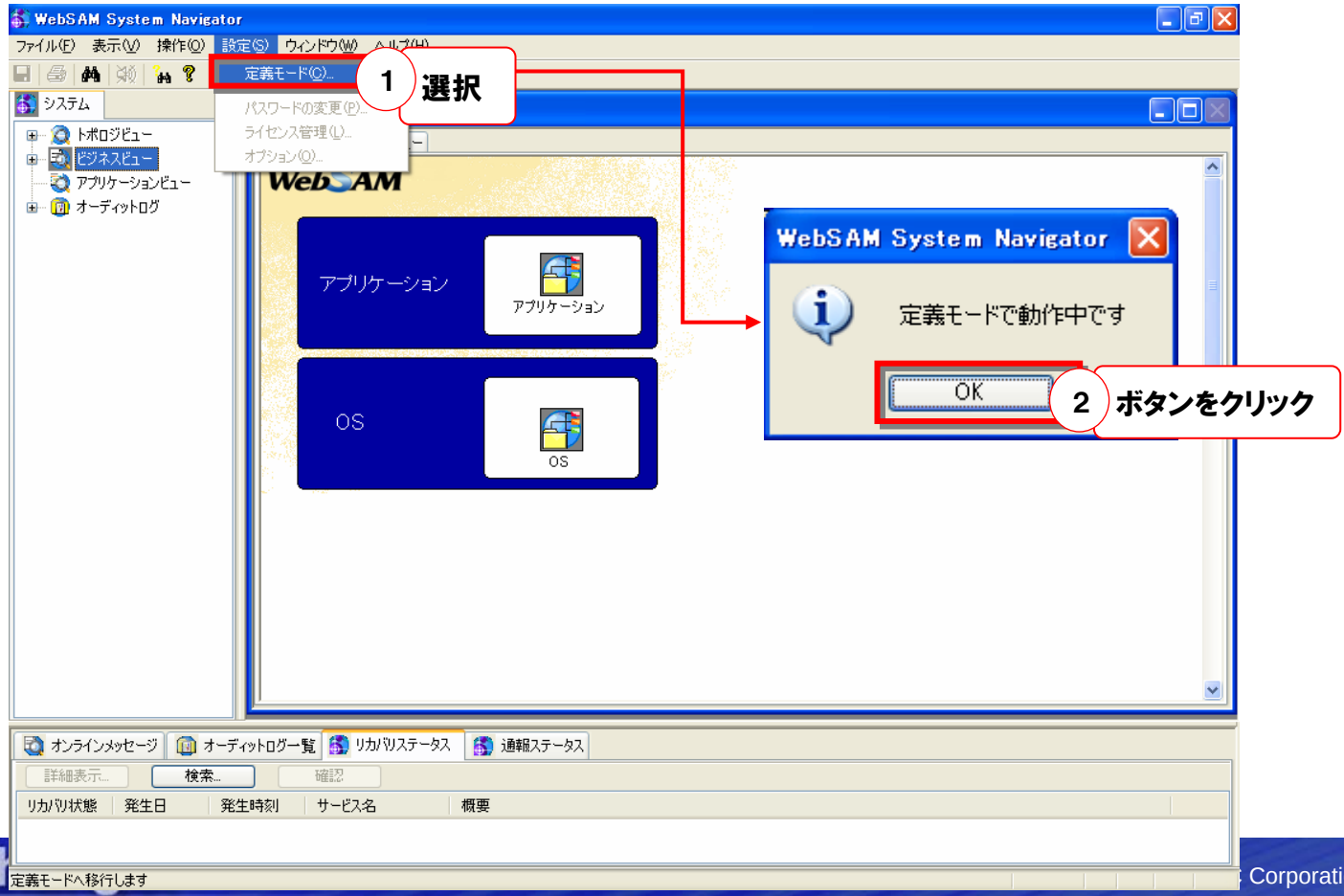
- デスクトップ上にあるWebSAM System Navigator Consoleのアイコンをダブルクリックし、System Navigatorを起動する。
  （または、「スタート」-「プログラム」-「WebSAM System Navigator」-「WebSAM System Navigator Console」からも起動できる。）



© NEC Corporation 2008

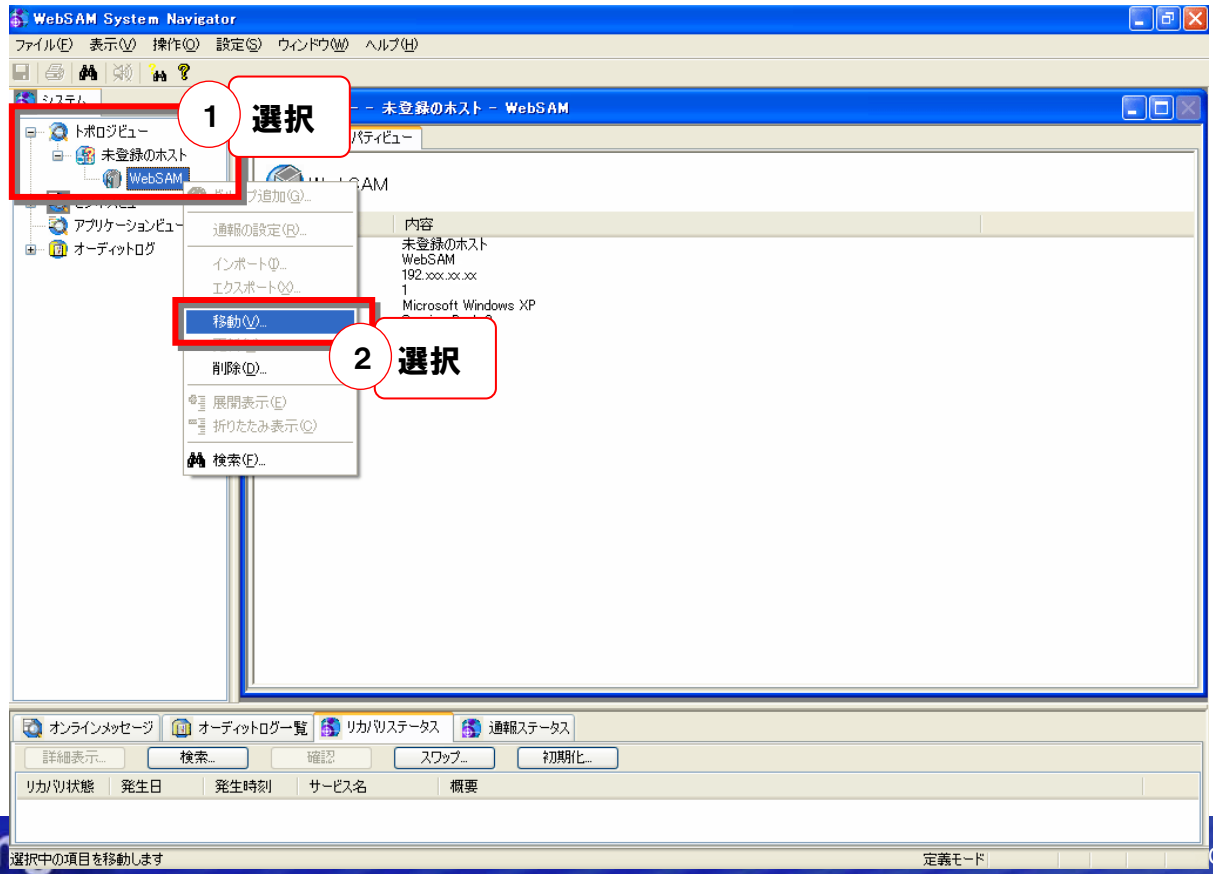
3．2 WebSAM System Navigatorの動作モード変更

- 監視画面で、メニューバーの「設定」-「定義モード」を選択して、動作モードを定義モードにする。
  確認画面が表示されるので、「OK」を押下する。
  ※「定義モード」とは、WebSAM System Navigatorの監視定義を行うためのモードです。



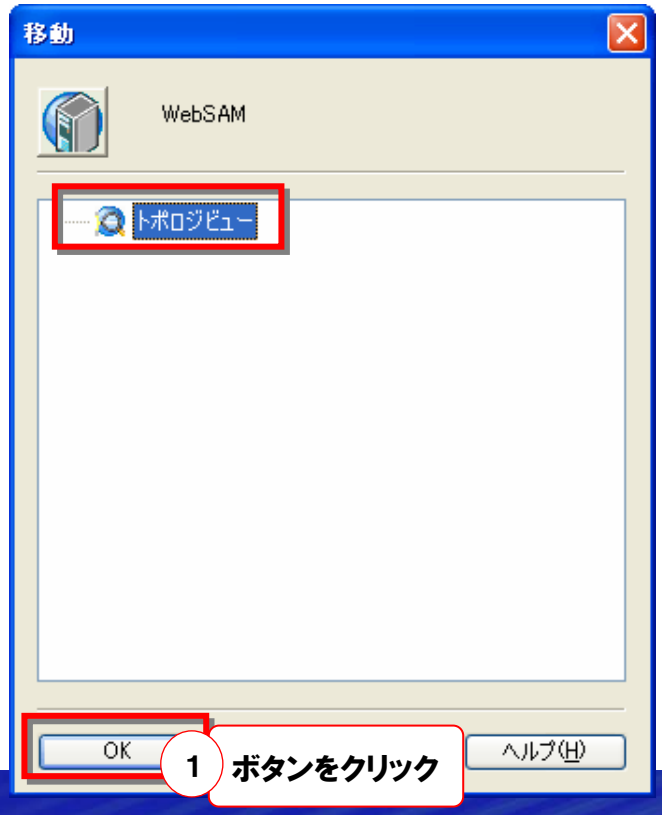
3．3 WebSAM System Navigatorのホスト移動

- 「システム」内の「トポロジビュー」-「未登録のホスト」を選択する。
  「未登録のホスト」階層下のサーバ名を右クリックし、「移動」を選択する。
  ※「未登録のホスト」配下には、ネットワークにつながっているWebSAM System Navigator Agentがインストールされているサーバ名が表示されます。
  ※「未登録のホスト」階層から移動させることで、登録されたホストとして認識されます。



3．4 WebSAM System Navigatorのホスト移動

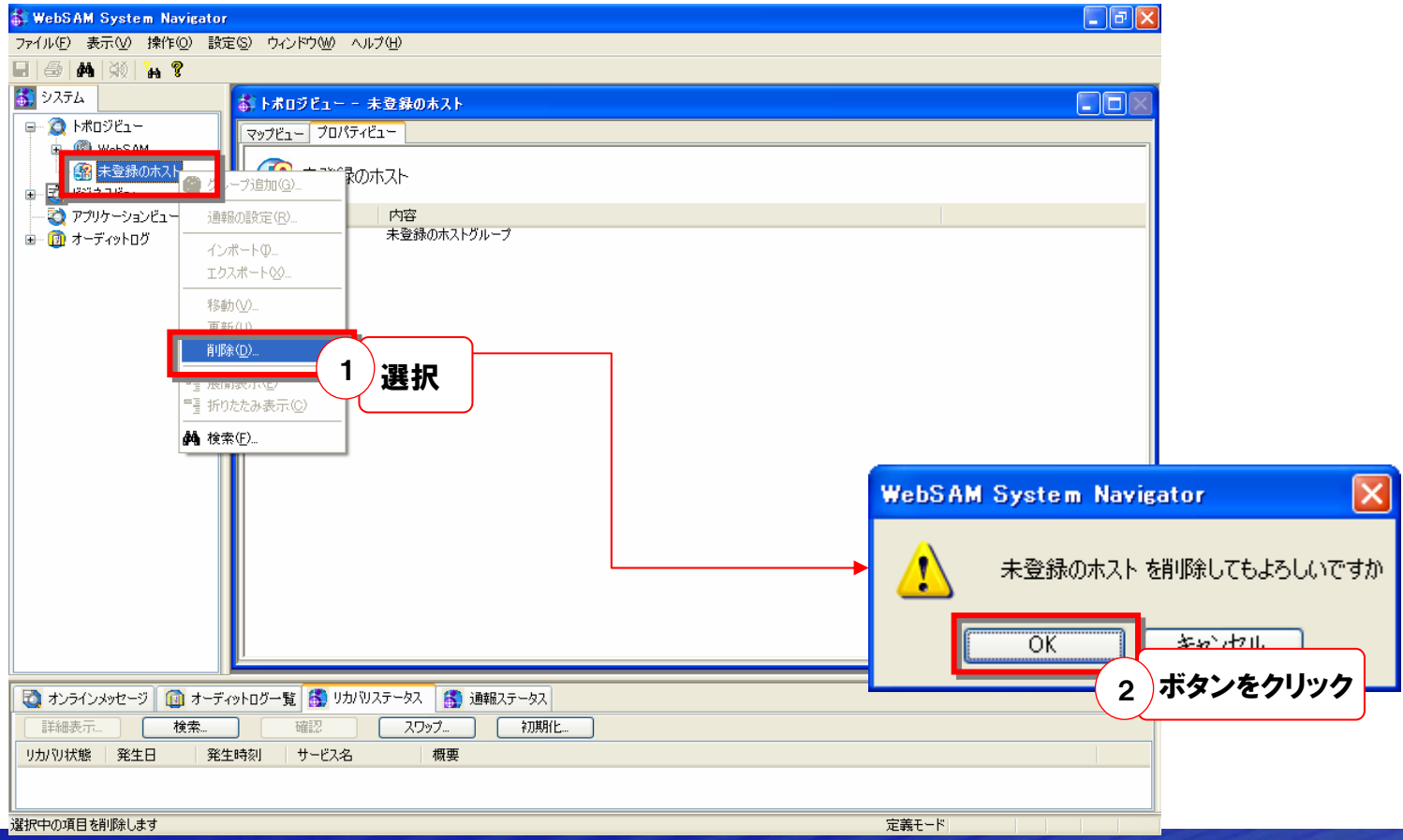
- 「移動」画面が表示されるので、「OK」を押下する。
  （またはドラッグ＆ドロップすることでも、移動できる。）
  ※デフォルトで、「トポロジビュー」が選択されているので、「OK」を押下することで、一つ上の階層に移動する。
  上記の作業を続けて、「未登録のホスト」内のサーバをすべて移動させる。



© NEC Corporation 2008

3．5 WebSAM System Navigatorのホスト移動

- 「未登録のホスト」階層化に、ホストが存在しないことを確認し、「未登録のホスト」を右クリックし、「削除」を選択する。
  確認画面が表示されるので、「OK」をクリックする。
  以上で、WebSAM System Navigatorの初期設定は終了です。



© NEC Corporation 2008

4. 重要度の設定

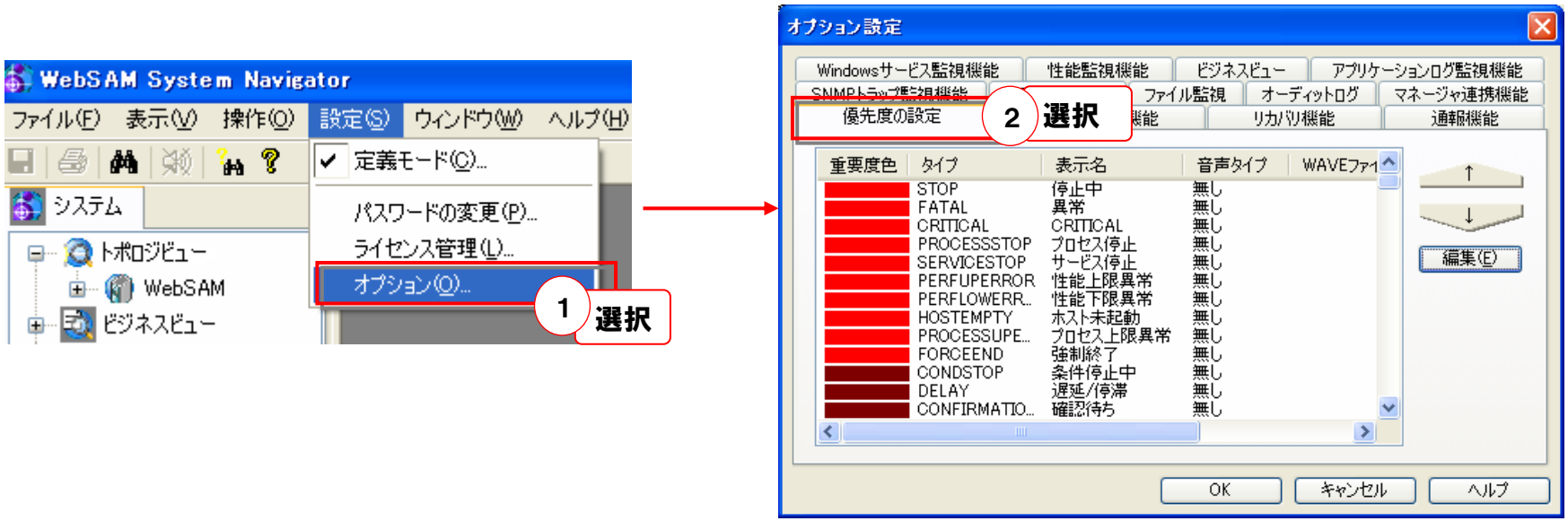
WebSAM System Navigatorで、メッセージを識別するための重要度の設定手順を明記します。

© NEC Corporation 2008

4．1 重要度の新規作成

Chakraのアラートの重要度のうち「Information」のみ、WebSAM System Navigatorには対応するものがデフォルトで存在しないたため、重要度を新規に作成する必要があります。下記に手順を記載いたします。

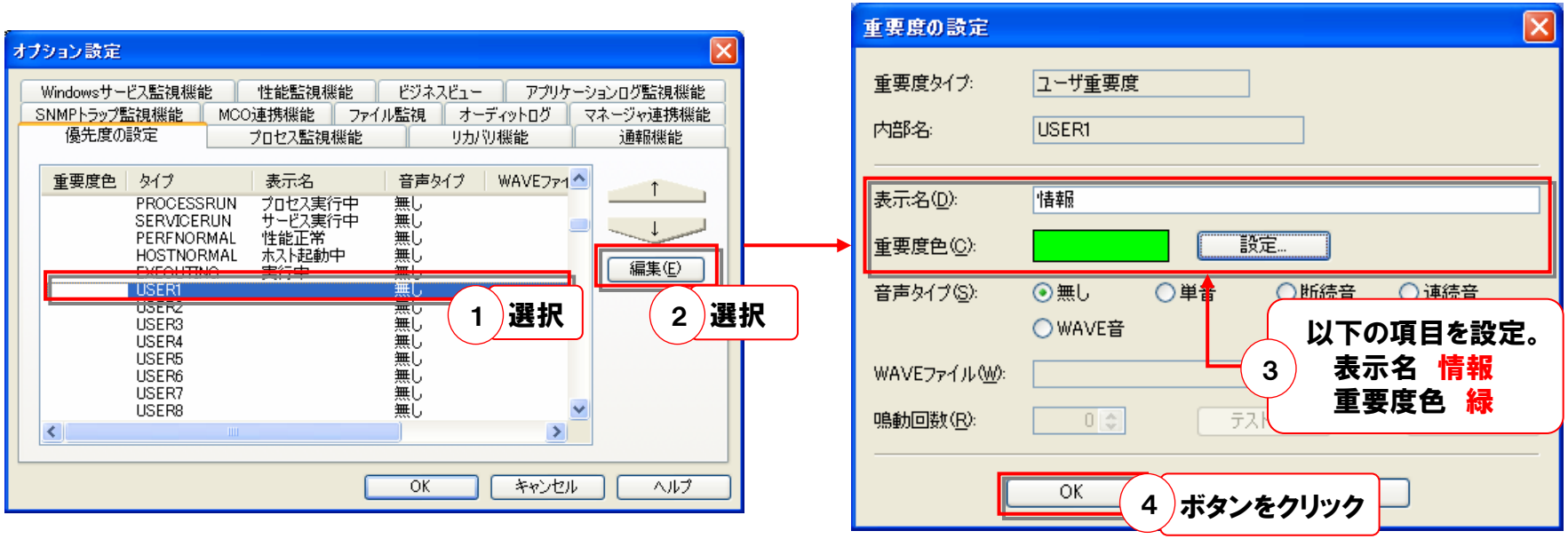
- 定義モードであることを確認後、メニューバーの「設定」ー「オプション」を選択する。
  「オプション設定」画面が表示されるので、「優先度の設定」タブを選択する。



© NEC Corporation 2008

4．2 重要度の新規作成

- 「優先度の設定」内にあるタイプ「USER1」を選択して、「編集」を押下する。
  「重要度の設定」画面が表示されるので、以下の項目を設定する。



© NEC Corporation 2008

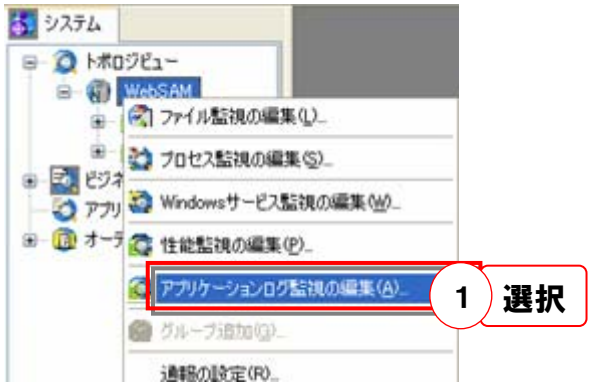
5. トポロジビューの設定

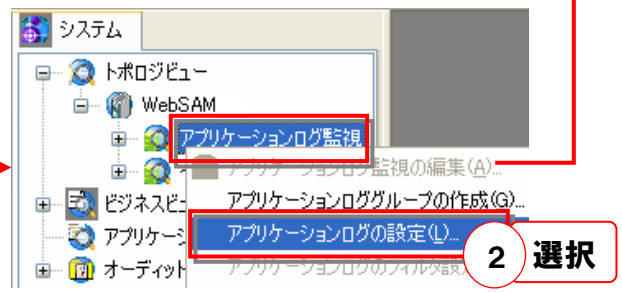
WebSAM System Navigatorで、アプリケーションログを監視するための設定手順を明記します。

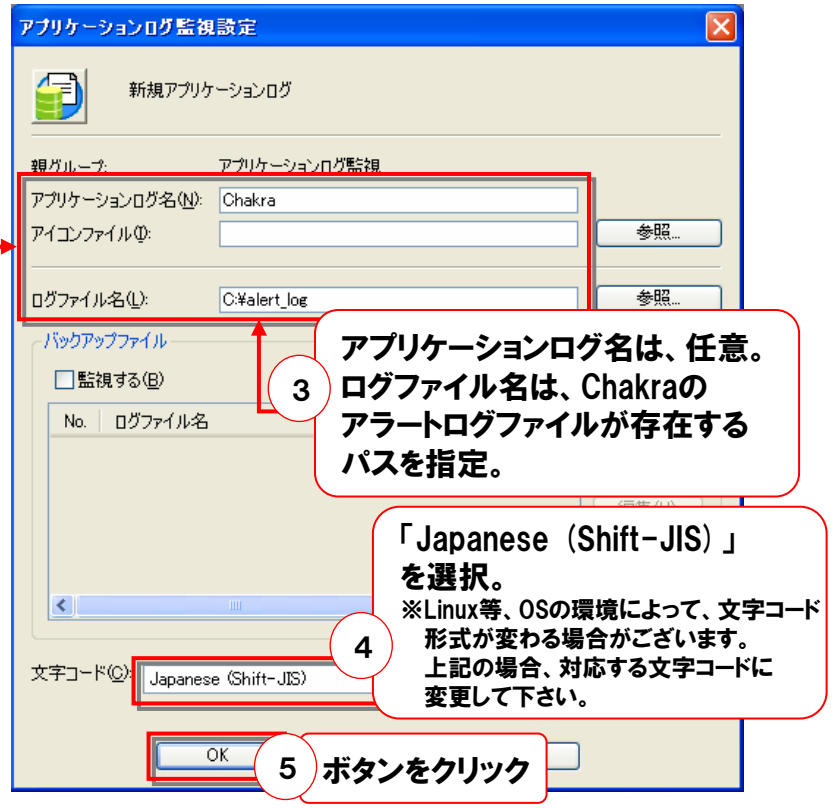
© NEC Corporation 2008

5．1 アプリケーションログの設定

- 定義モードであることを確認後、トポロジービュー内にある対象ホスト選択して、右クリックメニューから、「アプリケーションログ監視の編集」を選択する。
  トポロジービュー内にある「アプリケーションログ監視」を選択して、右クリックメニューから、「アプリケーションログの設定」を選択する。
  「アプリケーションログ監視設定」画面が表示されるので、以下の項目を設定する。



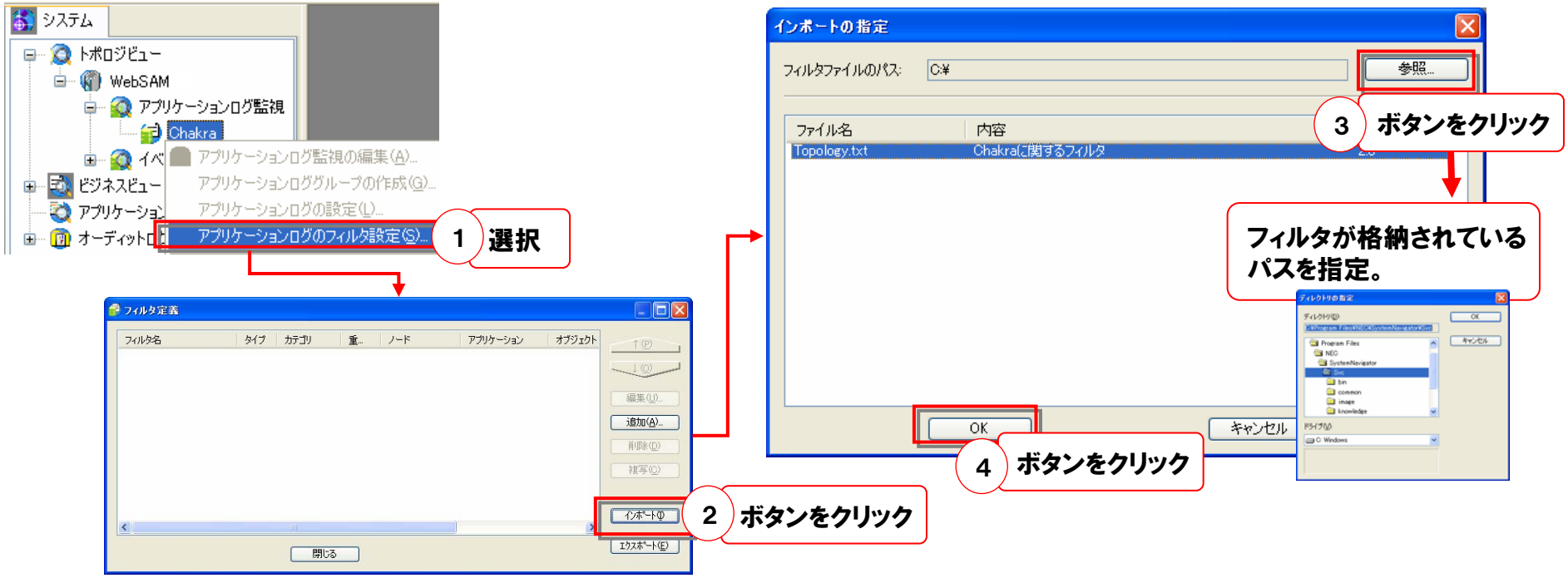




© NEC Corporation 2008

5．2 フィルタのインポート

- 作成したアプリケーションログを選択して、右クリックメニューから「アプリケーションログのフィルタ設定」を選択する。フィルタ定義画面が表示されるので、「インポート」を押下する。
  「インポートの指定」画面が表示されるので、インポートするフィルタが格納されているファイルパスを指定する。
  インポート可能なファイル名の一覧が表示されるので、対象のファイル（Topology.txt）を選択して、「OK」を押すと、フィルタがインポートされる。



© NEC Corporation 2008

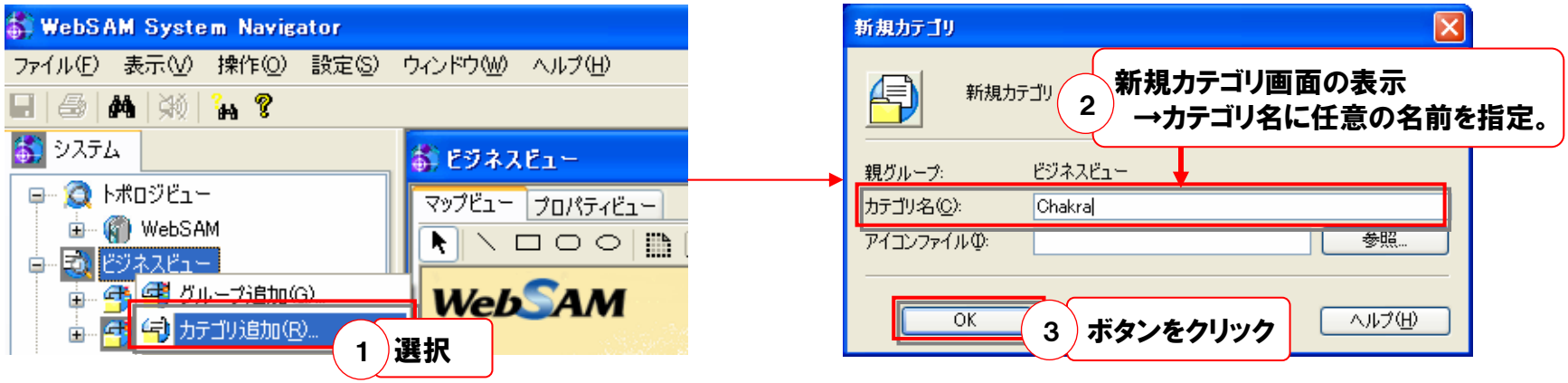
6. ビジネスビューの設定

WebSAM System Navigatorに起きたエラーを、表示させるための設定をします。
フィルタをインポートすることにより設定完了です。

© NEC Corporation 2008

6．1 カテゴリの作成

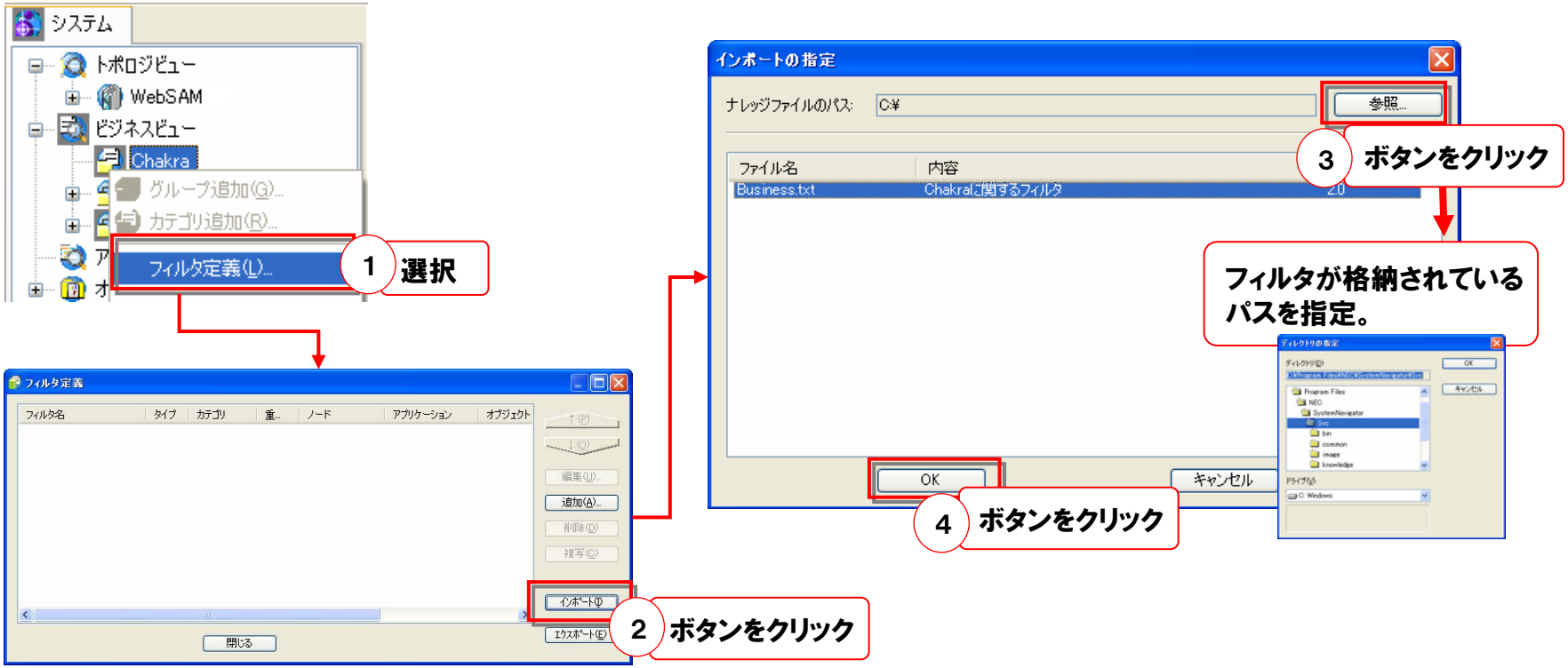
- 定義モードであることを確認後、ビジネスビューを選択して、右クリックメニューから「カテゴリ追加」を選択する。
  カテゴリ名（任意）を指定して、カテゴリを作成する。



© NEC Corporation 2008

6. 2 フィルタのインポート

- 作成したカテゴリを選択して、右クリックメニューから「フィルタ定義」を選択する。フィルタ定義画面が表示されるので、「インポート」を押下する。
  「インポートの指定」画面が表示されるので、インポートするフィルタが格納されているファイルパスを指定する。
  インポート可能なファイル名の一覧が表示されるので、対象のファイル(Business.txt)を選択して、「OK」を押すと、フィルタがインポートされる。

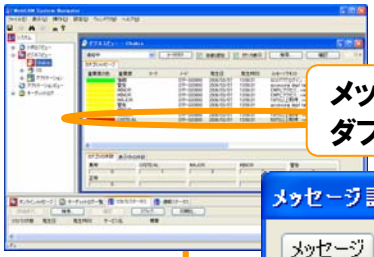


備考:メールやパトライトで通報する場合はヘルプを参照し通報設定を行ってください

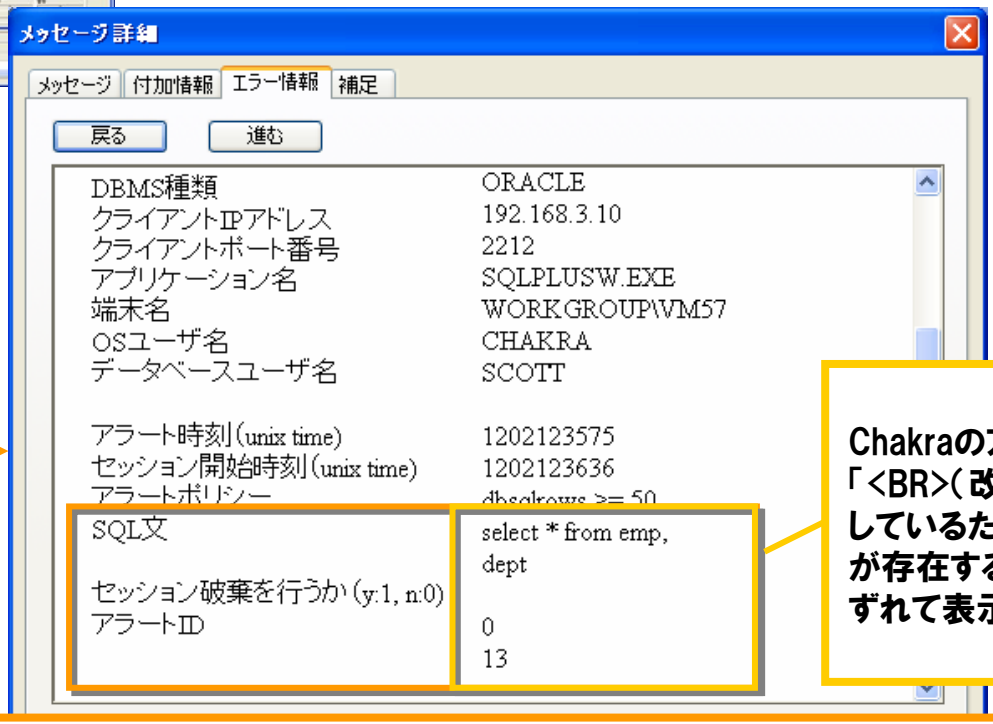
© NEC Corporation 2008

7. 注意事項

WebSAM System Navigator上で通知されたメッセージ確認を行う際、「メッセージ詳細」画面内にある「エラー情報」内の表示が、一部ずれることがございます。



メッセージを
ダブルクリック



Chakraのアラートログ内の「;(セミコロン)」を「
(改行)」に置換して、情報を表示しているため、SQL文内に、「;(セミコロン)」が存在する場合、SQL文以下の項目がずれて表示されてしまいます。

※上記の「エラー情報」内の表示は、
【標準標準ブラウザ:「Internet Explore 6.0 SP2」 標準設定フォント:「MS P ゴシック」】
の環境で、評価しております。
その他の環境では、表示が崩れる可能性がございます(フォントに依存しますのでご注意ください)

以上でChakra-WebSAM System Navigatorの
連携設定は完了となります

© NEC Corporation 2008

Empowered by Innovation